Machine Learning Text Classification and Natural Language Processing Approach to Cybersecurity Training Curriculum Analysis

August 2021

Team Boilermaker

Kevin Tian
Purdue University
West Lafayette, Indiana, USA
tian160@purdue.edu

Bengisu Cuneyit
Purdue University
West Lafayette, Indiana, USA
bcuneyit@purdue.edu

INL Mentor

Dr. Gary M. Deckard
gary.deckard@inl.gov

Abstract

In the domain of cybersecurity, there are a wide variety of education and training courses offered by a variety of training providers (commercial vendors, governmental, and academic institutions). Unfortunately, a comprehensive cross-provider mapping of the body of course offerings does not currently exist. Furthermore, although individual providers have made efforts, an accepted cross-provider mapping of education and training courses (or categories) to an accepted framework of work-roles by cybersecurity work-role and competency level has not yet been developed. The inability to compare training courses by topic or cybersecurity work-role and the level of difficulty (competency level) affects all organizations in identifying and selecting potential training opportunities for personnel performing cybersecurity duties.

In this work, we report on our application of Machine Learning (ML) Text Classification and Natural Language Processing (NLP) methodologies to begin to create a process to organize an accurate and thorough catalog of course offerings by work-role and competency level. Through the analysis of text-based course attributes (description, learning objectives, prerequisites, etc.), along with the text-based attributes for identified cybersecurity work-roles, our ML efforts examined methods to determine the work-role "best-fit" for each course, as well as the competency level through action-verb text comparison.

I. Table of Contents

II. Introduction

Many employees in the cybersecurity workforce today perform additional tasks outside the scope of their original job description. As the cybersecurity field evolves to encompass a wider variety of job duties, it becomes more difficult to hire the necessary workforce and train current employees for all tasks that they need to perform. Many positions in the cybersecurity workforce have common duties as well as other basic requirements, such as education and experience. This blurs the lines between distinct "specialized" jobs and limits growth opportunities within corporations, which in return can demotivate employees and discourage them from expanding their skillsets.

Organizations face numerous challenges in hiring cybersecurity talent as well as educating and training their cybersecurity workforce to meet the needed competency levels required for specific cybersecurity work-roles. Additionally, organizations struggle to understand the specific training needed for their workforce and to justify expenditure of training funds without comparative references between potential training offerings. A major factor is the lack of standardization in cybersecurity education and training standards for curriculum. This task is particularly difficult for the cybersecurity workforce tasked with protecting the Industrial Control Systems (ICS) systems that operate our nation's critical infrastructure.

In this work, we applied Machine Learning (ML) Text Classification methodologies to organize an accurate and thorough catalog of course offerings that establishes competency level equivalencies across providers. We theorized that it was possible to align the course offerings to an accepted framework of industry work-roles such as the National Institute for Standards & Technology (NIST) National Initiative for Cybersecurity Education (NICE) (Petersen, Santos, Smith, & Witte, 2020) by work-role and competency level. While the NIST NICE Framework does not include a work-role framework for ICS cybersecurity, joint research between Idaho National Laboratory (INL) and Idaho State University (ISU) has proposed standardized cybersecurity work-roles for the ICS field. As we discuss the goals of our project, consider that the discussion of "work-roles" includes those in ICS-related areas. To manually tag and label courses currently, courses must be categorized by subject matter experts or through expert analysis.

Training offerings across the cybersecurity field have associated course descriptions with specific text-based attributes for each course. Correspondingly, the NICE Framework and ISU-INL research driven ICS work-roles contain text-based descriptions and verbiage for their associated Tasks, Knowledge, and Skills (TKSs).[1]

The overall significance of our research lies in the novelty of utilizing ML to classify work-role frameworks and cybersecurity curriculum descriptions in a way whereby organizations which have assigned specific work-roles for their cybersecurity workforce can then identify appropriate training by work-role and competency level, regardless of provider or instructional method (Deckard, 2021).

[1] Skill and Ability statements from the previous NICE Framework version have been refactored for simplicity into Skill statements.

III. Related Work

Our project concept is grounded in recent course equivalency work by the Federal Emergency Management Agency (FEMA) and Argonne National Laboratory (ANL) to map course equivalencies for State, Local, Tribal & Territorial (SLTT) training courses to existing FEMA courses. This work relied upon decision science techniques such as multi-attribute utility theory (MAUT) (Jansen, 2011), Natural Language Processing (NLP) (IBM, 2020), and the concepts of ML text classification to understand the meaning of various text-based attributes for each course. Through this work, FEMA and ANL were able to create a Course Equivalency Tool (CET) to evaluate courses and assign equivalencies (Argonne National Laboratory, 2020). This tool uses a course equivalency model that measured the similarity of courses through three different approaches: course match, course methodology, and course topic.

Another work that contributed significantly to this project was the unpublished master's thesis work of Randall Jung, a research fellow at INL. Jung's work utilized the NICE framework to show how the federal government's General Schedule system (GS) failed to maintain currency, specifically for the GS-2210 job series. The NICE framework utilizes 'task,' 'knowledge,' and 'skill' statements in conjunction with 'work' and 'learner' concepts to categorize employee competencies and outline a standardized method of describing work-roles (Jung, 2020). Accompanying the master's thesis, Jung included a training course repository with cybersecurity courses manually categorized into NICE roles and Bloom's Taxonomy Levels (Armstrong, 2010), among other labels.

The Competency Health and Maturity Progression Model (Cyber-CHAMP) is a five-step model created and developed at INL to provide Cyber awareness and training to improve an organization's cyber efficiency (Hott, Stailey, Haderlie, & Ley, 2020). Cyber-CHAMP hopes to address the issue of organizations without a standardized communication framework, introducing the term 'cyber-hygiene'. The five steps include taking a snapshot of the organization's cyber hygiene, mapping the organization's job positions and job roles, having employees complete a task analysis worksheet, and producing training recommendations for employees based on their task analysis results, and reassessing the organization's cyber hygiene after a period of time.

Cyber-CHAMP includes a Task Analysis Tool, which prompts the user about various skills and tasks typically used in their work, eventually giving the user a breakdown of how their skills align within the context of the NICE framework. In addition to this breakdown, the tool also offers a list of manually aggregated cybersecurity training courses pertaining to an employee's areas of skill. The current methodology of course recommendation is a significant weakness within the Cyber-CHAMP tool, as this manual method will not scale well with the increase of courses, and the course list offered does not consider the user's competency level.

We believe many of these issues with the previous methodology can be rectified through a machine learning algorithm/script that will categorize cybersecurity courses and create an indexable catalog that will pair users with relevant cybersecurity courses for their specific competency level.

IV. Methodology

The data used in this paper primarily comes from Randall Jung's repository of cybersecurity courses included with the master's thesis (Jung, 2020). The repository is a Microsoft Excel workbook organized into different spreadsheets. The sheet we primarily focused on is the 'Trainings' sheet, where each training course was labeled by the course vendor, classification status, course number, course title, course description, Bloom's Taxonomy Level, etc. (For full spreadsheet see Table C1). In total, the dataset has 18 categories, with some of the data entries missing. These courses constituted the 'main dataset' of training courses our model trained on and was augmented by the manually aggregated course catalog currently used in the Cyber-CHAMP Task Analysis Tool.

Vendor	Classified	Course Number	Course Title	Course Description	Course Duration	Course Cost	Course Delivery	Course Location	Access Period	Competency Level
ISA		FG02	Mathematics for Instrumentation Technicians	This course is specifically designed for the instrument technician who may be struggling with mathematical computations or those who need a basic refresher. The course is focused entirely on fundamental problems and solutions that an instrument tech continuously works with from entry to supervisory level experience. It also provides a good prerequisite for the various math calculations involved in other ISA training courses.	4 days					Fundamentals
ISA		FG07	Intro to Industrial Processes, Measurement and Control	This popular course combines lecture and hands-on labs to provide an overview of industrial measurement and control. Technicians, engineers, and managers are provided with a foundation for communication with other control system professionals. Serves as a solid fundamental course for introduction to other ISA courses.	4.5 days	$3,855	Live			Fundamentals
ISA		FG05E	Fundamentals of Industrial Process Measurement & Control	This self-paced, online course provides an overview of industrial measurement and control for technicians, engineers, and managers providing a basic understanding and foundation for communication with other control systems professionals.	12 weeks	$1,800	Online	Online		Fundamentals
ISA		FG15E	Developing and Applying Standard Instrumentation and Control Documentation	This course will present the methodology for the designing and developing of control systems documentation. The development of piping and instrument diagrams (P&IDs) and related ISA drawings are emphasized. This course covers both the development and the reading/interpreting of these documents, making it beneficial to engineers, designers, software programmers, system integrators, and technicians.	2 days		Live			Novice

Figure 1: 'Trainings' spreadsheet in Randall Jung's repository of cybersecurity courses

In the process to organize cybersecurity courses, we treated each course as a 'document,' allowing our process to closely align to traditional document classification techniques within the NLP space. Due to time constraints and the popularity of Naïve Bayes (NB) and Support Vector Machines (SVM) in document classification tasks, we decided on these two to be our primary classifiers of interest.

The project is broken into two phases for implementation, namely Phase 1 and Phase 2.

A. Phase 1

Phase 1 will be responsible for classifying cybersecurity courses into the five competency levels defined in the Cyber-CHAMP model. These competency levels are Novice, Fundamentals, Intermediate, Advanced, and Expert. In the Jung repository, course competency level was prelabeled and assigned to their respective courses, allowing us to skip manually labeling courses to their proper competency levels. In this approach, each row in the repository had its column data aggregated into one text paragraph, minus the value from the 'Course Competency' column. This data was then split into a tuple, with the first entry being the raw text and the second entry the value of the course competency.

In this approach, we vectorized the raw text into a Term Frequency – Inverse Document Frequency vector (TF-IDF) and applied the Multinomial Naïve Bayes (MultinomialNB) and Stochastic

Gradient Descent (SGD) classifiers provided by Python package Scikit-learn to our data. SGD is a simple and efficient approach to fit linear classifiers and regressors, which in our case is SVM.

B. Phase 2

Phase 2 will be responsible for attributing NICE work-roles to the courses through Cosine Similarity (Prabhakaran, 2020) and Euclidian Distance (D'Agostino, 2009). Due to the utilization of TF-IDF and vectors to represent a document's text, we chose Cosine Similarity and Euclidian Distance as similarities between vectors that represent text, serving as a proxy for textual similarity. Cosine Similarity is a commonly used technique to match similar documents and its approach focuses on the maximum number of common words between documents. Euclidean Distance, which is the shortest distance between two points, is a measure used to neutralize inaccurate Cosine Similarity outputs that occur when the number of common words increase as the size of a document increases, regardless of the document topics. When plotted on a multi-dimensional space, where each dimension corresponds to a word in the document, the Cosine Similarity captures the orientation (the angle) of the documents and the Euclidean distance computes the magnitude (Prabhakaran, 2020).

In this approach, information about the NICE work-roles and their respective TKSs were compiled each into one 'document', one for each NIST work-role. The raw text is then cleaned and stored in a Python 'list.' For each document in the Python list, stop words such as 'the' and 'a' are removed and the subsequent text is then vectorized using the vectorizer from Scikit-learn into TF-IDF vectors. The same process is repeated for the training course data, and the similarity is calculated through 'cosine_similarity' and 'euclidian_distances' methods from Scikit-learn. The results are then stored within a similarity matrix, and the most relevant documents can then be retrieved.

V. Results and Discussion

A. Phase 1: Naïve Bayes (NB) & Support Vector Machines (SVM) Approach

1. Accuracy

Both classifiers are commonly used in text/document classification due to their relatively high accuracy, but it was somewhat surprising to see that both NB and SVM Classifiers hovering around 50% accuracy. To evaluate accuracy, we considered the True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). Accuracy is calculated as:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

The NB classifier had a 47.05% accuracy, and the SVM classifier had a 54.90% accuracy. Once we optimized the model hyperparameters with the GridSearch package from scikit-learn, we were able to achieve a 66.83% accuracy with NB, and an accuracy of 88.08% for SVM. For the NB

classifier, a classifier considered as one of the best document classifiers (Ting, Ip, & Tsang, 2011), it yielded surprisingly low accuracy even with optimized hyperparameters. Due to SVM having a higher accuracy compared to the NB classifier, we chose to proceed with SVM for the rest of our model.

2. Interpretation of Confusion Matrix

A confusion matrix is used to evaluate the quality of the output of a classifier on a dataset. High values along the diagonal indicate correct classification, and high values on the non-diagonal entries signal misclassification (the model's predicted label is different from the true label). We can see this visually with the color of the tile, as darker colored tiles indicate a greater accuracy.

The intersection of a row and a column in a confusion matrix represents the percentage correctly classified between labels. In Figure 2 below, the intersection between the Fundamentals labels is at 31.37%. This shows that out of the predicted Fundamentals labels, 31.37% were the true label of Fundamentals.

In Figure 2, we can see the Naïve Bayes classifier is having trouble accurately classifying Intermediate, Expert, and Advanced labels, while it is able to classify Fundamentals and Novice labels with reasonable success. The NB classifier is having trouble distinguishing between the Novice and Intermediate labels and is classifying them as Fundamentals.

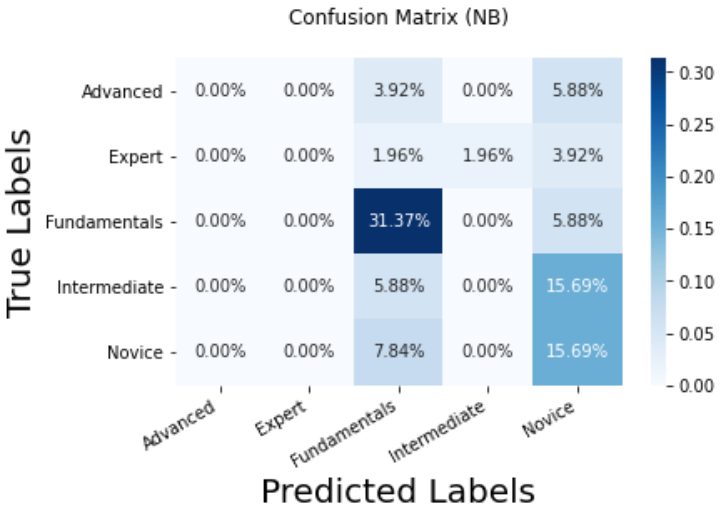

Figure 2: Naïve Bayes Confusion Matrix

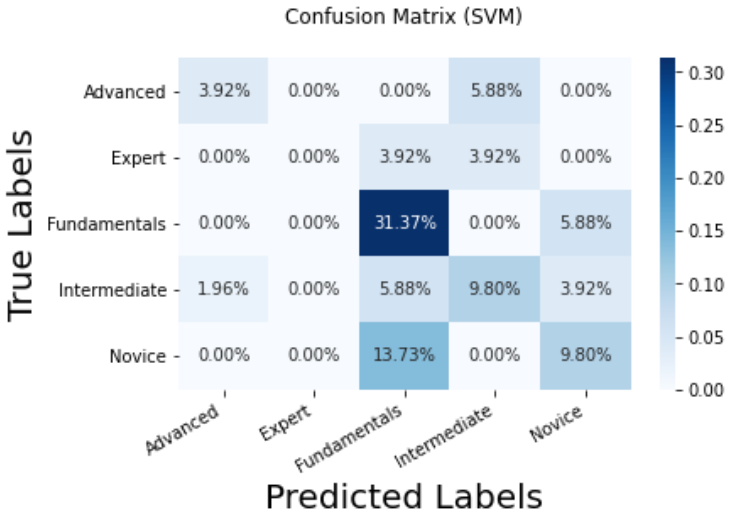

Figure 3: Support Vector Machines Confusion Matrix

We can see in Figure 3 the SVM classifier is able to classify the Fundamentals label considerably well, and it is having trouble distinguishing between the pairing of Fundamentals & Novice and Fundamentals & Intermediate. Like the Naïve Bayes classifier, it is having a difficult time classifying Expert labels, having a 0% accuracy overall.

B. Phase 2: Cosine Similarity & Euclidean Distance

Due to time constraints and the nature of the dataset, accuracy metrics would most likely prove unhelpful in validating our model due to the sheer number of labels and the fact each course can have multiple NICE work-roles as labels.

An alternative approach to quantifying how well this model performed is outlined in the section for future work.

While we were not able to generate a quantifiable metric of how well our model performed, our model does seem to provide its intended functionality, as shown in the figure below.

```
Document: Is a high level introductory course designed to expose participants to the challenges and frameworks used in implemen
ting and sustaining a cyber security program at a nuclear and/or radiological facility.  The course uses the National Institute
of Standards and Technology (NIST) cyber security framework as the course structure for conveying the core concepts and compone
nts of a cyber security program.  This includes, identifying sources of risk, protection of digital systems, detection concepts
should protection fail, response to detection points, and recovering the system back to conditions before a cyber event.
Similar Documents:

Out[28]: {'roles': ['ovmgt001 : 60.22%',
  'prcda001 : 51.55%',
  'sprsk001 : 50.87%',
```

Figure 4: Support Vector Machines Confusion Matrix

In Figure 4, we can see the document is returning a list of NICE role abbreviations with Cosine Similarity serving as a proxy for how relevant the NICE role is to the course (Refer to Figure C1 for the full output). The example course description's key phrase "…implementing and sustaining a cyber security [sic] program at a nuclear and/or radiological facility."

In the NICE role descriptions spreadsheet, the role ‘ovmgt001’ returns the following description:

> *Information Systems Security Manager- Responsible for the cybersecurity of a program, organization, system, or enclave.*

This seems to closely match the description of what skills the example course would like the user to learn.

Searching for the role with the lowest Cosine Similarity, ‘coclo002’, which had a Cosine Similarity of 9.06% (Not pictured in Figure 4, available in Figure C1), returned a position with the description of:

> *All Source-Collection Manager – Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.*

This position description does not seem to align with the course’s goals, which suggests our model is working correctly.

VI. Conclusions

Through the combination of Phase 1 and Phase 2 approaches, our model pipeline can receive general characteristics of a cybersecurity course, and successfully categorize the course into the proper competency level and return the associated NICE work-roles with Cosine Similarity serving as a proxy for percent match for relevancy. Our code has been modularized into a singular python script named ‘b_script.py’ and can be used within other tools to classify courses.

Figure 5 demonstrates how our script works. The script can receive a course’s description along with any other attributes of the course, and now can return a python dictionary with the competency level and the relevant NICE roles as output, all within one model (full output available in Figure C2).

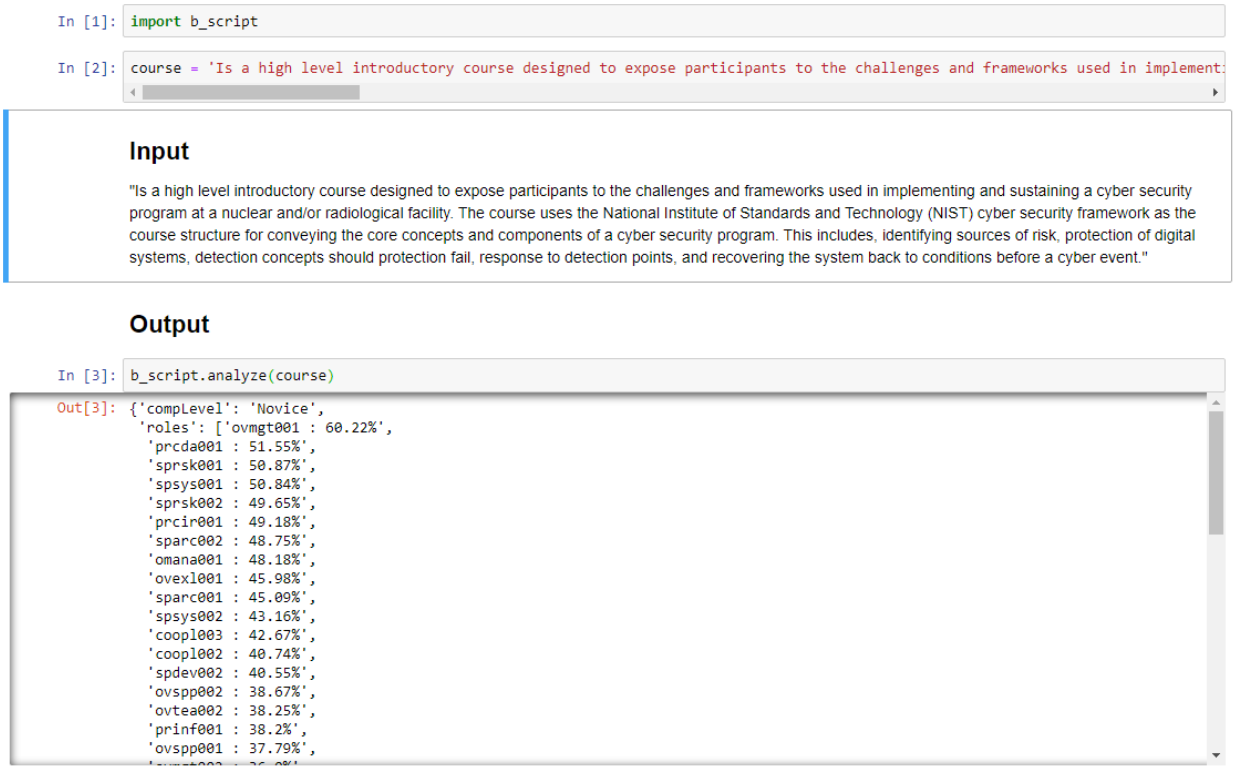

Figure 5: Working example of model classification and output

While the results are preliminary due to a limited dataset, our approach shows document classification through NLP techniques such as SVM and NB is possible and should be further investigated as an alternative to the manual and subjective classification of training courses present in the industry today. Automation of course classification comes with many benefits. Automation reduces the need for manual labor, offers a more objective approach to classification, can deal with large amounts of data quickly, and offers a flexible solution that can be used by many industries regardless of unique workforce constraints—provided a standardization framework such as NICE exists within that industry.

VII. Future Work

Utilizing methods such as NB, SVM, Cosine Similarity, and Euclidean Distance, our approach yielded promising results. An alternative implementation geared towards optimizing the model and increasing the accuracy is to use new transformer-based architectures, namely Google's Bidirectional Encoder Representations from Transformers (BERT), to generate context-based word embeddings, allowing the model to also consider locations of words within a sentence to see if this yields better results.

The logical next step for this project is to run the aggregated training course data through the script and build a repository of training courses with their predicted competency level as well as the

NICE roles with the percent similarity included. This will be the ‘indexable’ course catalog mentioned previously.

In the future, we intend to integrate our indexable course catalog with the Cyber-CHAMP Task Analysis Survey, allowing Cyber-CHAMP users to find courses that match their competency level as well as their work-role description. The Cyber-CHAMP Task Analysis Tool will assess a user’s competency and most relevant NICE role. The tool can then search based on those criteria, producing a list of relevant courses for the user using our indexable course catalog.

Another point of interest for future work is to determine a way to calculate the ‘cut-off’ point for relevancy. This is because, at a certain point, the NICE work-roles returned from our script begins to not accurately describe the input course at all.

As mentioned previously in the results section, a proposed approach to quantifying the performance of the Cosine Similarity and Euclidian Distance model is to use a weighted score for each course categorized and cross-referencing the predictions to the correct NICE roles on the ‘Work-Role to Training Map’ spreadsheet in Jung’s repository. Our original training dataset did not have the NICE roles labeled, so this alternative approach can address this issue.

Finally, we would also like to aggregate more training course data. For the majority of the project, we did not have access to enough clean data to effectively reach a conclusion, so the collection of more course data will further legitimize our results.

VIII. References

Argonne National Laboratory. (2020). Enterprise Wide Assessment of Courses: Analysis of FEMA’s State, Local,Tribal, and Territorial Training Courses. FEMA.

Armstrong, P. (2010). *Bloom's Taxonomy*. Retrieved from Vanderbilt University: https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

D'Agostino, M. (2009, August). *What's so special about Euclidean distance? A characterization with applications to mobility and spatial voting.* Retrieved from researchgate: https://www.researchgate.net/publication/258222305_What's_so_special_about_Euclidean_distance_A_characterization_with_applications_to_mobility_and_spatial_voting

Deckard, G. M. (2021, Feb). Classification Predictive Models for Course Equivalency Analysis of CybersecurityEducation and Training Curricula. *2021 2nd Quarter LDRD Seed Proposal*. Idaho National Laboratory.

Hott, J. A., Stailey, S. D., Haderlie, D. M., & Ley, R. F. (2020). Extending the National Initiative for Cybersecurity Education (NICE) Framework Across Organizational Security. *National CyberWatch Center Digital Press*, 7-17.

Howard, J., & Ruder, S. (2018). Universal Language Model Fine-tuning for Text Classification. *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics*

(Volume 1: Long Papers), *1*, pp. 328-339. Retrieved from https://academic.microsoft.com/paper/2963026768

IBM. (2020, July 2). *Natural Language PRocessing (NLP)*. Retrieved from IBM: https://www.ibm.com/cloud/learn/natural-language-processing

Jansen, S. J. (2011). *The Measurement and Analysis of Housing Preference and Choice.* Springer, Dordrecht.

Jiawei Han, M. K. (2012). Getting to Know Your Data. In *Data Mining (Third Edition)* (pp. 39-82). Morgan Kaufmann.

Jung, R. (2020, April). Challenges for the General Schedule 2210 Series. *Unpublished*. USAF Air War College .

Luo, X. (2021). Efficient English text classification using selected Machine Learning Techniques. *Alexandria Engineering Journal*, 3401-3409.

McKinney, W. (2010). Data Structures for Statistical Computing in Python. In *Proceedings of the 9th Python in Science Conference* (pp. 56-61).

Pedregosa, F. (2011). *Confusion Matrix.* Retrieved from Scikit-learn: https://scikit-learn.org/stable/auto_examples/model_selection/plot_confusion_matrix.html

Pedregosa, F. (2011). *Naive Bayes*. Retrieved from Scikit-learn: https://scikit-learn.org/stable/modules/naive_bayes.html

Pedregosa, F. (2011). *Support Vector Machines*. Retrieved from Scikit-learn: https://scikit-learn.org/stable/modules/svm.html

Pedregosa, F. (2011). *Tuning the hyper-parameters of an estimator*. Retrieved from Scikit-learn: https://scikit-learn.org/stable/modules/grid_search.html

Petersen, R., Santos, D., Smith, M., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE framework).* National Institute of Standards and Technology.

Prabhakaran, S. (2020, October 11). *Cosine Similarity – Understanding the math and how it works (with python codes)*. Retrieved from Machine Learning Plus: https://www.machinelearningplus.com/nlp/cosine-similarity/

Ting, S. L., Ip, W. H., & Tsang, A. H. (2011). Is Naïve Bayes a Good Classifier for Document Classification? *International Journal of Software Engineering and Its Applications Vol. 5, No. 3*.

Varun. (2020, September 26). *Calculating Document Similarities using BERT, word2vec, and other models*. Retrieved from Towards Data Science: https://towardsdatascience.com/calculating-document-similarities-using-bert-and-other-models-b2c1a29c9630

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A – COSTAR Analysis and 5-Minute Brief

Customer: Who are the intended customers, and what are their important unmet needs?

We hope to serve any industry that has workforce development and training through courses in the cybersecurity space. Our tool will address the "Jack of all trades, master of none." issue in the cybersecurity workforce where employees are in charge of many tasks that don't particularly fall into the scope of their position. This reduces job specialization and employees' task competency considerably.

Opportunity: What is the full size of the opportunity?

We have the potential to create the first tool to index training courses across the cybersecurity industry by work-role and competency level. This tool could also be extended to any industry with an existing standardized work-role framework.

Solution: What is your proposed solution for capturing the opportunity?

We are proposing an indexable course catalog of cybersecurity courses to NIST/NICE and ICS work-role mapping. We have compiled our code including our model into a singular Python script as we are working on implementation of a catalog that can be utilized as a tool. Our mode can be integrated the into Cyber-CHAMP's Task Analysis Tool—giving employees more insightful results on their specific course needs than the current tool. We have also documented our code for readability and replication, keeping possible future improvement efforts in mind.

Team: Who needs to be on your team to ensure your solution's success?

The team currently includes two juniors from Purdue University; Kevin Tian who is double majoring in Data Science and Applied Statistics, and Bengisu Cuneyit who is majoring in Computer Science and minoring in Mathematics, as well as our mentor Dr. Gary M. Deckard from INL.

Our team's technical background was a big contributor in our impressive preliminary results and promising conclusions. We hope to continue this project throughout fall and spring if we can receive the needed funding. We would also like to add more interns to the team who have similar backgrounds in order to make the project larger in scale and streamline some of the work.

Advantage: What is your solution's competitive advantage over alternatives?

Current Industry Approach	Our Approach
× Manual tagging of courses through Subject Matter Experts	✓ Automatic tagging of courses through Machine Learning
× Model is subjective and classification can differ between experts	✓ An objective approach to classifying courses
× Is not scalable for a large number of courses, will require large amount of manual labor	✓ Can handle large inputs of courses through our model pipeline

× Some approaches can only be applied to a single industry due to initial work needed to set up	✓ Flexible and can apply to industries outside of the cybersecurity space (medical, business, etc.)

Results: What results will be achieved from your solutions?

By offering the correct courses to employees, we will try to encourage work-role awareness and increase specialization in the workforce by solving the previously mentioned 'Jack of all trades…' problem.

Our project is also a chance for INL to be recognized as the first organization to introduce such a tool into the cybersecurity space. This could get our names out as pioneers in the industry and create a good amount of positive exposure for the laboratory. INL's eminence will also increase through the publication of an article on our project in an IEEE Research Journal.

Appendix B – Code Repository

Unless stated otherwise, the original format of the code are Jupyter Notebook style code blocks.

Demo Notebook for modularized code

```
#!/usr/bin/env python
# coding: utf-8

# In[1]:


import b_script


# In[2]:


course = 'Is a high level introductory course designed to expose participants to the challenges and frameworks used in implementing and sustaining a cyber security program at a nuclear and/or radiological facility.  The course uses the National Institute of Standards and Technology (NIST) cyber security framework as the course structure for conveying the core concepts and components of a cyber security program.  This includes, identifying sources of risk, protection of digital systems, detection concepts should protection fail, response to detection points, and recovering the system back to conditions before a cyber event.'


# ## Input
# "Is a high level introductory course designed to expose participants to the challenges and frameworks used in implementing and sustaining a cyber security program at a nuclear and/or radiological facility.  The course uses the National Institute of Standards and Technology (NIST) cyber security framework as the course structure for conveying the core concepts and components of a cyber security program.  This includes, identifying sources of risk, protection of digital systems, detection concepts should protection fail, response to detection points, and recovering the system back to conditions before a cyber event."

# ## Output

# In[3]:


b_script.analyze(course)

```

Modularized Phase 1 and Phase 2 Code (Python Script)

```

#!/usr/bin/env python
# coding: utf-8

# In[6]:


import pandas as pd
import numpy as np

from sklearn.feature_extraction.text import CountVectorizer
from sklearn.feature_extraction.text import TfidfTransformer
from sklearn.linear_model import SGDClassifier
from sklearn.pipeline import Pipeline
```

```
import pickle
from sklearn.model_selection import GridSearchCV



from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.metrics.pairwise import cosine_similarity
from sklearn.metrics.pairwise import euclidean_distances

import re

# In[9]:




# In[12]:


#train


# In[7]:


def analyze(courseDesc):
    train = pd.read_csv('train.csv')
    test = pd.read_csv('test.csv')
    train = train.sample(frac =1)
    count_vect = CountVectorizer()
    X_train_counts = count_vect.fit_transform(train.data)
    tfidf_transformer = TfidfTransformer()
    X_train_tfidf = tfidf_transformer.fit_transform(X_train_counts)

    text_clf_svm = Pipeline([('vect', CountVectorizer()), ('tfidf', TfidfTransformer()), ('clf-svm',
SGDClassifier(loss='perceptron', penalty='l2',alpha=1e-3, random_state=42)),])
    _ = text_clf_svm.fit(train.data, train.target)
    predicted_svm = text_clf_svm.predict(test.data)
    # np.mean(predicted_svm == test.target)
    # rslts['(Before) SVM'] =np.mean(predicted_svm == test.target)
    parameters_svm = {'vect__ngram_range': [(1,1), (1,2)], 'tfidf__use_idf': (True, False), 'clf-svm__alpha': (1e-2, 1e-3),}
    gs_clf_svm = GridSearchCV(text_clf_svm, parameters_svm, n_jobs=-1)
    gs_clf_svm = gs_clf_svm.fit(train.data, train.target)


    testdf = pd.DataFrame({'data': [courseDesc],})
    testdf.columns = ['data']
    count_vect = CountVectorizer()
    inf = count_vect.fit_transform(testdf.data)
    shp = list(inf.shape)

    compLevel = list(gs_clf_svm.predict(testdf.data))[0]

    outDict = {}
    outDict['compLevel']= compLevel
    ## Cosine Similarity

    new = pd.read_csv('cleaned_nice_ksas.csv')
    coursedf = pd.DataFrame([courseDesc])
    coursedf.columns = ['descriptions']
    new = coursedf.append(new)
    tfidfvectoriser=TfidfVectorizer()
    tfidfvectoriser.fit(new.descriptions)
    tfidf_vectors=tfidfvectoriser.transform(new.descriptions)

    pairwise_similarities=np.dot(tfidf_vectors,tfidf_vectors.T).toarray()
```

```
    pairwise_differences=euclidean_distances(tfidf_vectors)

    def most_similar(doc_id,similarity_matrix,matrix):
        roles = []
#         print (f'Document: {new.iloc[doc_id]["descriptions"]}')
#         print ('\n')
#         print ('Similar Documents:')
        if matrix=='Cosine Similarity':
            similar_ix=np.argsort(similarity_matrix[doc_id])[::-1]
        elif matrix=='Euclidean Distance':
            similar_ix=np.argsort(similarity_matrix[doc_id])
        for ix in similar_ix:
            if ix==doc_id:
                continue
            regex = r"[a-zA-Z]{5}\d{3}"
            roles.append(f'{re.findall(regex, new.iloc[ix]["descriptions"])[0]} : {round(similarity_matrix[doc_id][ix]*1000, 2)}%')
        outDict['roles'] = roles
            #print (f'Document: {new.iloc[ix]["descriptions"]}')
            #print (f'{matrix} : {similarity_matrix[doc_id][ix]}')

    most_similar(0,pairwise_similarities,'Cosine Similarity')
    #most_similar(0,pairwise_differences,'Euclidean Distance')
    return outDict


# In[3]:









# In[5]:









# In[ ]:
```

Cleaning Jung dataset for course to NICE Work-role mapping

```
#!/usr/bin/env python
# coding: utf-8

# In[158]:


import pandas as pd
import numpy as np
import string
import re
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.feature_extraction.text import TfidfTransformer
from nltk.corpus import stopwords
from nltk.tokenize import word_tokenize
```

```
15.
16.
17.  # In[159]:
18.
19.
20.  data = pd.read_csv('jungdsfull.csv')
21.
22.
23.  # In[160]:
24.
25.
26.  data = data.drop(['Classified'], axis = 1)
27.
28.
29.  # In[161]:
30.
31.
32.  data.fillna("No", inplace = True)
33.
34.
35.  # In[162]:
36.
37.
38.  data = data.drop(['Link', 'Learning Path', 'Learning Path Name'], axis = 1)
39.
40.
41.  # In[163]:
42.
43.
44.  data
45.
46.
47.  # In[164]:
48.
49.
50.  data = data.applymap(lambda x: x.lower())
51.
52.
53.  # In[165]:
54.
55.
56.  data = data.applymap(lambda x : x.translate(str.maketrans('', '', string.punctuation)))
57.
58.
59.  # In[166]:
60.
61.
62.  data = data.applymap(lambda x: " ".join(x.split()))
63.
64.
65.  # In[167]:
66.
67.
68.  data
69.
70.
71.  # ## Assembly into one document & saving to CSV, only needs to be run once
72.  # ]
73.
74.  # In[168]:
75.
76.
77.  # documents = []
78.
79.
80.  # In[169]:
```

```
81.
82.
83.  # for i in range(0, data.shape[0]):
84.  #     txt = " ".join(data.loc[i].to_list())
85.  #     tokens_without_sw = [word for word in word_tokenize(txt) if not word in stopwords.words()]
86.  #     documents.append(" ".join(tokens_without_sw))
87.
88.
89.  # In[170]:
90.
91.
92.  # documents[1]
93.
94.
95.  # In[171]:
96.
97.
98.  # docs = pd.DataFrame(documents)
99.  # docs.columns = ['docs']
100. # docs.to_csv('cleaned_docs.csv', index = False)
101.
102.
103. # In[172]:
104.
105.
106. docs = pd.read_csv('cleaned_docs.csv') #.drop('Unnamed: 0', axis =1)
107.
108.
109. # In[173]:
110.
111.
112. docs
113.
```

Handling Cyber-CHAMP Dataset, Jung Dataset, and implementation of Naïve Bayes & SVM Classifiers:

```
1.   #!/usr/bin/env python
2.   # coding: utf-8
3.
4.   # In[49]:
5.
6.
7.   import numpy as np
8.   import pandas as pd
9.   import matplotlib.pyplot as plt
10.  from sklearn.feature_extraction.text import CountVectorizer
11.
12.
13.  # In[50]:
14.
15.
16.  data = pd.read_excel(io = "jung.xlsx", sheet_name = "Trainings", engine='openpyxl')
17.
18.
19.  # In[51]:
```

```
20.
21.
22.  data.shape
23.
24.
25.  # In[52]:
26.
27.
28.  data.columns
29.
30.
31.  # In[53]:
32.
33.
34.  print(data['Competency Level'].count())
35.  print(data['Competency Level'].isna().sum())
36.  data = data[data['Competency Level'].notna()]
37.  print(data['Competency Level'].isna().sum())
38.
39.
40.  # In[54]:
41.
42.
43.
44.  data['Competency Level'] = data['Competency Level'].str.strip()
45.  data['Competency Level'].unique()
46.
47.
48.  # In[55]:
49.
50.
51.  counts = data['Competency Level'].value_counts().to_list()
52.  print(data['Competency Level'].value_counts())
53.  cat = tuple(data['Competency Level'].value_counts().index.to_list())
54.
55.
56.  # In[56]:
57.
58.
59.  cat
60.
61.
62.  # In[57]:
63.
64.
65.  dlist = data.values.tolist()
66.
67.
68.  # In[58]:
69.
70.
71.  fig, ax = plt.subplots()
72.  ax.bar(cat, counts)
73.  fig.autofmt_xdate()
74.  plt.show()
75.
76.
77.  # In[59]:
78.
79.
80.  proc_entries = []
81.
82.  for i in dlist:
83.      comp = i[11]
84.      i.pop(11)
85.      string = " ".join(str(x) for x in i)
```

```
86.       string = " ".join(str(x) for x in (list(string.replace('nan', '').split())))
87.       proc_entries.append((string, comp))
88.       #print(i[11])
89.
90.
91.   # In[60]:
92.
93.
94.   proc_entries[-1] = (proc_entries[-1][0],'Expert')
95.   proc_entries[-2] = (proc_entries[-2][0],'Expert')
96.
97.
98.   # In[61]:
99.
100.
101. proc_entries[-1]
102.
103.
104. # In[62]:
105.
106.
107. # fig, ax = plt.subplots()
108. # ax.bar(cat, counts)
109. # fig.autofmt_xdate()
110. # plt.show()
111. adj_cat = list(cat)
112. adj_cat.pop(5)
113. counts.pop(5)
114. counts[4] = 11
115.
116.
117. # In[63]:
118.
119.
120. fig, ax = plt.subplots()
121. ax.bar(adj_cat, counts)
122. fig.autofmt_xdate()
123. plt.show()
124.
125.
126. # ### Cyber Champ Dataset
127.
128. # In[64]:
129.
130.
131. import re
132. import functools
133.
134.
135. # In[65]:
136.
137.
138. data = open("CyberCHAMP.txt", "r")
139. rawtext = data.read()
140.
141. courses = re.split("(?<!\S)\d\|(?!C)", rawtext)
142.
143.
144. # In[66]:
145.
146.
147. my_list = []
148.
149. for course in courses:
150.     fixed_course = course.replace("|", " ")
151.     fixed_course = fixed_course.replace("\n", " ").replace("•", " ").replace("●", " ")
```

```
    fixed_course = fixed_course.split()
    fixed_course = " ".join(fixed_course)
    my_list.append(fixed_course)


# In[67]:


for i in my_list:
    print(i + '\n')


# In[68]:


competency = [i.split()[0] for i in my_list]
competency.remove("ICS")
print(competency)


# In[69]:


new_list = [i.split(' ', 1) for i in my_list]
for x in new_list:
    print(x)


# In[70]:


for i in new_list:
    if i[0] == 'Design':
        i[0] = 'Expert'


# In[71]:


astuple = []
for i in new_list:
    astuple.append((i[1], i[0]))

astuple.pop(0)


# In[72]:


test = pd.DataFrame(astuple)


# In[73]:


#test.loc[1]['data']


# In[74]:


test


# ### Naive Bayes

```

```
# In[75]:



# In[76]:


train = pd.DataFrame(proc_entries)


# In[77]:


train.columns = ['data', 'target']
train = train.sample(frac = 1) ##Shuffle dataframe


# In[78]:


count_vect = CountVectorizer()
X_train_counts = count_vect.fit_transform(train.data)
X_train_counts.shape


# In[79]:


from sklearn.feature_extraction.text import TfidfTransformer
tfidf_transformer = TfidfTransformer()
X_train_tfidf = tfidf_transformer.fit_transform(X_train_counts)
X_train_tfidf.shape


# In[80]:


from sklearn.naive_bayes import MultinomialNB
clf = MultinomialNB().fit(X_train_tfidf, train.target)


# In[81]:


from sklearn.pipeline import Pipeline
text_clf = Pipeline([('vect', CountVectorizer()), ('tfidf', TfidfTransformer()),('clf', MultinomialNB()),])
text_clf = text_clf.fit(train.data, train.target)


# In[82]:


test.columns = ['data', 'target']
test = test.sample(frac = 1)

predicted = text_clf.predict(test.data)
np.mean(predicted == test.target)


rslts = {'(Before) Naive Bayes': np.mean(predicted==test.target),}


# ### SVM

# In[83]:
```

```
284.
285.
286. from sklearn.linear_model import SGDClassifier
287.
288. text_clf_svm = Pipeline([('vect', CountVectorizer()), ('tfidf', TfidfTransformer()), ('clf-svm', SGDClassifier(loss='perceptron',
     penalty='l2',alpha=1e-3, random_state=42)),])
289. _ = text_clf_svm.fit(train.data, train.target)
290. predicted_svm = text_clf_svm.predict(test.data)
291. np.mean(predicted_svm == test.target)
292. rslts['(Before) SVM'] =np.mean(predicted_svm == test.target)
293.
294.
295. # ### Using Gridsearch (SVM)
296.
297. # In[84]:
298.
299.
300. from sklearn.model_selection import GridSearchCV
301.
302.
303. # In[85]:
304.
305.
306. parameters_svm = {'vect__ngram_range': [(1,1), (1,2)], 'tfidf__use_idf': (True, False), 'clf-svm__alpha': (1e-2, 1e-3),}
307.
308.
309. # In[86]:
310.
311.
312. gs_clf_svm = GridSearchCV(text_clf_svm, parameters_svm, n_jobs=-1)
313. gs_clf_svm = gs_clf_svm.fit(train.data, train.target)
314. print(gs_clf_svm.best_score_)
315. print(gs_clf_svm.best_params_)
316.
317. rslts['(Best Score) SVM']= gs_clf_svm.best_score_
318.
319.
320. # ## Saving SVM Model
321.
322. # In[87]:
323.
324.
325. # 1st method
326.
327.
328. # In[88]:
329.
330.
331. #from joblib import dump, load
332.
333.
334. # In[89]:
335.
336.
337. #dump(gs_clf_svm, 'gs_clf_svm.joblib')
338.
339.
340. # In[90]:
341.
342.
343. #clf = load('gs_clf_svm.joblib')
344.
345.
346. # In[91]:
347.
348.
```

```
#clf.predict(testdf.data)


# In[92]:


# 2nd method


# In[93]:


import pickle

pickle.dump(gs_clf_svm, open('clf_model.sav', 'wb'))


# In[94]:


clf = pickle.load(open('clf_model.sav', 'rb'))


# In[96]:


clf.predict(test.data)


# ### Using Gridsearch (NB)

# In[ ]:


parameters = {'vect__ngram_range': [(1,1), (1,2)], 'tfidf__use_idf': (True, False), 'clf__alpha': (1e-2, 1e-3),}


# In[ ]:


gs_clf = GridSearchCV(text_clf, parameters, n_jobs=-1)
gs_clf = gs_clf.fit(train.data, train.target)
print(gs_clf.best_score_)
print(gs_clf.best_params_)
rslts['(Best Score) Naive Bayes'] = gs_clf.best_score_


# ### Results

# In[ ]:


from sklearn import metrics


# In[ ]:


print(rslts)

#print(metrics.classification_report(test.target,pred_gs_svm))


# In[ ]:
```

```
svm_matrix = metrics.confusion_matrix(test.target,predicted_svm)
nb_matrix = metrics.confusion_matrix(test.target,predicted)


# ### Inference

# In[ ]:


testdf = pd.DataFrame({'data': ['Remember FG07- Intro to Industrial Processes, Measurement and Control ISA $3,855 Live; 4.5 days 3.2 CEU’s This popular course combines lecture and hands-on labs to provide an overview of industrial measurement and control. Technicians, engineers, and managers are provided with a foundation for communication with other control system professionals. Serves as a solid fundamental course for introduction to other ISA courses.', 'Design', 'Maintain','Remember'],})


# In[ ]:


testdf.columns = ['data']


# In[ ]:


count_vect = CountVectorizer()
inf = count_vect.fit_transform(testdf.data)
shp = list(inf.shape)


#
# ____
#
# <em><strong>'Remember FG07- Intro to Industrial Processes, Measurement and Control ISA $3,855 Live; 4.5 days 3.2 CEU’s This popular course combines lecture and hands-on labs to provide an overview of industrial measurement and control. Technicians, engineers, and managers are provided with a foundation for communication with other control system professionals. Serves as a solid fundamental course for introduction to other ISA courses.'</em></strong>
#
#
# > Should return 'Fundamentals'

# In[ ]:


list(text_clf_svm.predict(testdf.data))[0]


#
# ___
#
#
# <em><strong>'Design'</em></strong>
#
# > Should return 'Expert'

# In[ ]:


list(text_clf_svm.predict(testdf.data))[1]


#
# ---
#
# <em><strong>'Maintain'</em></strong>
#
```

```
#
# > Should return 'Intermediate'

# In[ ]:


list(text_clf_svm.predict(testdf.data))[2]


#
# ---
#
# <em><strong>'Remember'</em></strong>
#
# > Should return 'Fundamentals'

# In[ ]:


list(text_clf_svm.predict(testdf.data))[3]


# In[ ]:


import seaborn as sns


# In[ ]:


target_names = list(text_clf_svm.classes_)
svm_matrix


# In[ ]:




# In[ ]:


fig, ax = plt.subplots()

sns.heatmap(svm_matrix/np.sum(svm_matrix), fmt='.2%', cmap='Blues', annot =True, ax=ax, square = False)
ax.set_xlabel('Predicted Labels', fontsize = 20)
ax.set_ylabel('True Labels', fontsize = 20)
ax.set_title('Confusion Matrix (SVM)', pad=20)
ax.xaxis.set_ticklabels(target_names)
ax.yaxis.set_ticklabels(target_names)
fig.autofmt_xdate()
plt.yticks(rotation=360)
plt.show()


# In[ ]:


fig, ax = plt.subplots()

sns.heatmap(nb_matrix/np.sum(nb_matrix), fmt='.2%', cmap='Blues', annot =True, ax=ax)
ax.set_xlabel('Predicted Labels', fontsize = 20)
ax.set_ylabel('True Labels', fontsize = 20)
ax.set_title('Confusion Matrix (NB)', pad=20)
```

```
ax.xaxis.set_ticklabels(target_names)
ax.yaxis.set_ticklabels(target_names)
fig.autofmt_xdate()
plt.yticks(rotation=360)
plt.show()
```

Cleaning Cyber-CHAMP Dataset

```
import pandas as pd
import numpy as np
import re
import functools
data = open("CyberCHAMP.txt", "r")
rawtext = data.read()

courses = re.split("(?<!\S)\d\|(?!C)", rawtext)
my_list = []

for course in courses:
    fixed_course = course.replace("|", " ")
    fixed_course = fixed_course.replace("\n", " ").replace("•", " ").replace("●", " ")
    fixed_course = fixed_course.split()
    fixed_course = " ".join(fixed_course)
    my_list.append(fixed_course)

for i in my_list:
    print(i + '\n')

competency = [i.split()[0] for i in my_list]
competency.remove("ICS")
print(competency)
new_list = [i.split(' ', 1) for i in my_list]
for x in new_list:
    print(x)
for i in new_list:
    if i[0] == 'Design':
        i[0] = 'Expert'
astuple = []
for i in new_list:
    astuple.append((i[1], i[0]))
astuple[1:]

```

NIST NICE Work-role cleaning

```
#!/usr/bin/env python
# coding: utf-8

# In[38]:


import pandas as pd
import numpy as np
import json
import re


```

```
# In[ ]:



# ## Preprocessing

# In[39]:


df = pd.read_csv("tasks.csv")

# In[40]:


df = df.transpose().reset_index()

# In[41]:


df.columns = list(df.loc[0])

# In[42]:


df = df.drop(0)

# In[43]:


df2 = pd.read_csv('role2task.csv')

# In[44]:


df2.head()

# ## Course Dataset

# In[45]:


courses = pd.read_csv('course dataset.csv')

# In[46]:


courses.columns = ['entries']

# In[47]:


courseList = list(courses.entries)

# In[48]:


```

```
79.
80.  courseList
81.
82.
83.  # ## Text cleaning conversion to dictionary format
84.
85.  # In[49]:
86.
87.
88.  adjList = []
89.
90.
91.
92.
93.  # In[50]:
94.
95.
96.  ## So the last entry in courseList is the "]" so its not actually an entry
97.  for a in range(0,len(courseList)-1):
98.      print(a)
99.      mt = re.search('\[.+\]', courseList[a])
100.     temp = courseList[a].replace(mt.group(), "")
101.     temp = temp.replace(",\"relatedRoleIds:\"", "")
102.     temp = temp[:-22]+"}"
103.     temp = temp.replace('false', '"False"')
104.     temp = temp.replace('true', '"True"')
105.     temp = temp.replace('""', '"None"')
106.     roles = mt.group()
107.     roles = roles.replace(" ", "")
108.     roles = roles.replace("\"", "")
109.     roles = roles.replace('[', "")
110.     roles = roles.replace(']', "")
111.     roles = roles.replace(',', " ")
112.     y=json.loads(temp)
113.     y['roles'] = roles.split(" ")
114.     adjList.append(y)
115.
116.
117. # In[51]:
118.
119.
120. adjList[3]
121.
122.
123. # In[52]:
124.
125.
126. pd.DataFrame(adjList)
127.
128.
129. # ## Creating Role dictionary
130.
131. # In[53]:
132.
133.
134. roles = pd.read_csv('role2task.csv')
135.
136.
137. # In[54]:
138.
139.
140. workRoles = list(roles['Work Role ID'])
141.
142.
143. # In[55]:
144.
```

```
145.
146. for i in range(0, len(workRoles)):
147.     workRoles[i] = workRoles[i].strip()
148.
149.
150. # In[56]:
151.
152.
153. workRoles
154.
155.
156. # In[57]:
157.
158.
159. categories=workRoles.copy()
160. workRoles.insert(0, 'text')
161.
162.
163. # In[58]:
164.
165.
166. workRoles
167.
168.
169. # In[59]:
170.
171.
172. tempDict = {}
173. for i in workRoles:
174.     tempDict[i] = [0]
175.
176. pd.DataFrame.from_dict(tempDict)
177.
178.
179. # In[60]:
180.
181.
182. def cleantxt(text):
183.     return text
184.
185.
186. # In[61]:
187.
188.
189. p = []
190. for i in adjList:
191.     currentRoles = i['roles']
192.     txt = ''
193.     i.pop('AdvTrURL', None)
194.     for x in i.keys():
195.         if x is not 'roles':
196.             txt = txt + i[x] +' '
197.     temp2=tempDict.copy()
198.     for j in currentRoles:
199.
200.         temp2[j] = [1]
201.
202.     txt = txt.split()
203.     temp2['text'] = " ".join(txt)
204.
205.     p.append(temp2)
206.
207.
208. # In[62]:
209.
210.
```

```
p[0]


# In[63]:


tempDF = pd.DataFrame()
for i in p:
    tempDF = tempDF.append(pd.DataFrame(i))

tempDF = tempDF.reset_index().drop(['index'], axis =1)


# ## Saves the data as CSV

# In[76]:


##tempDF.to_csv('fixed_data.csv')


# In[64]:


```

Appendix C – Detailed Figures & Results

Vendor	Classified	Course Number	Course Title	Course Description	Course Duration	Course Cost	Course Delivery	Course Location	Access Period	Competency Level
ISA		FG02	Mathematics for Instrumentation Technicians	This course is specifically designed for the instrument technician who may be struggling with mathematical computations or those who need a basic refresher. The course is focused entirely on fundamental problems and solutions that an instrument tech continuously works with from entry to supervisory level experience. It also provides a good prerequisite for the various math calculations involved in other ISA training courses.	4 days					Fundamentals
ISA		FG07	Intro to Industrial Processes, Measurement and Control	This popular course combines lecture and hands-on labs to provide an overview of industrial measurement and control. Technicians, engineers, and managers are provided with a foundation for communication with other control system professionals. Serves as a solid fundamental course for introduction to other ISA courses.	4.5 days	$3,855	Live			Fundamentals
ISA		FG05E	Fundamentals of Industrial Process Measurement & Control	This self-paced, online course provides an overview of industrial measurement and control for technicians, engineers, and managers providing a basic understanding and foundation for communication with other control systems professionals.	12 weeks	$1,800	Online	Online		Fundamentals
ISA		FG15E	Developing and Applying Standard Instrumentation and Control Documentation	This course will present the methodology for the designing and developing of control systems documentation. The development of piping and instrument diagrams (P&IDs) and related ISA drawings are emphasized. This course covers both the development and the reading/interpreting of these documents, making it beneficial to engineers, designers, software programmers, system integrators, and technicians.	2 days		Live			Novice
ISA		TC05	Tuning Control Loops	This course is directed to anyone who would like to gain a better understanding of how to tune control loops-whether they have tuned loops but would like to become more proficient or they have never tuned a loop before. Registrants are expected to have a basic understanding of instrumentation and controls (either by working experience or taking fundamental courses such as ISA's FG07: Introduction to Industrial Automation and Control) as this course does not cover that material.	3 days	$3,790	Live			Novice
ISA		TC10	Troubleshooting Instrumentation and Control Systems	This course presents a systematic approach to troubleshooting and start-up of single- and multi-loop control loops. You'll see how pressure, level, flow, and temperature loops operate to maintain good process control systems. Knowledge of instrumentation and control is assumed.	2 days	$3,790	Live			Novice
ISA		EC05	Designing and Tuning Feedback and Advanced Regulatory Control Strategies	The required field of knowledge of a process control engineer has expanded significantly in recent years. What once was limited to measurement technology, signal transmission and feedback control has now expanded to include alarm management, safety instrumented systems, integration of automation and business systems, plus a host of other technologies. Good process control techniques are still as important as ever. This course will provide the foundation which will allow a process control engineer to make appropriate use of all technologies available. For those who select or design process control strategies, this course also provides a thorough background in feedback control, plus a working knowledge of the application of advanced regulatory control strategies such as ratio, cascade, feed forward, override and decoupling. The course emphasizes the benefits of advanced regulatory control for improving the economics of process operations.	3 days		Online	Online		Novice
ISA	Yes	ES10E	Applying Instrumentation in Hazordous Locations	This self-paced, online course provides a systematic approach to specifying and implementing instrumentation in hazardous locations. Related standards from National Fire Protection Association (NFPA), National Electrical Manufacturers Association (NEMA), International Electrotechnical Commission (IEC), American Petroleum Institute (API), and ISA are discussed.	8 weeks	$1,440 - $1,800	Online, Instructor-Assisted	Online		Intermediate
ISA		IC40E	Batch Control Using the ANSI/ISA88 Standards	This course presents an approach to developing functional requirements/specifications using the models and terminology defined in the ANSI/ISA88 batch control standards. A review of the characteristics of batch manufacturing systems is included. Participants will explore the ANSI/ISA88 concept that separates the recipe from the equipment. This course includes a methodology that defines an object approach based on ANSI/ISA88 that promotes the reuse of these objects from one project to the next.	3 days		Live			Expert
ISA		IC55E	Implementing Business to MES Integration Using the ANSI/ISA95 Standards	This course introduces the fundamental concepts of the ANSI/ISA95 standards so that students can apply them to implementing an integration between plant manufacturing systems and business systems. By understanding the object models and information flows defined in the ANSI/ISA95 standards, you will have the tools you need to specify, design, and execute a successful business to manufacturing integration project. This course is ideal for Integration Project Managers; Manufacturing Information Systems Analysts; Information Design Engineers and IT Professionals.	7 weeks	$1,440 - $1,800	Online, Instructor-Assisted	Online		Intermediate
ISA		EN00V	Control Systems Engineering (CSE) PE Exam Review Course	This course reviews the knowledge and skills areas that are included in the Control Systems Engineer (CSE) Professional Engineer (PE) examination produced by the National Council of Examiners for Engineering and Surveying (NCEES) and administered by the US state professional license boards each October. The intent of the class is to prepare an engineer with four or more years of experience to take the exam by providing instruction in the broad range of technical areas that will be tested. The content is based on the CSE Exam Specification that went into effect in October 2011.			Virtual Instructor-Led	Online		Expert
ISA		EC51VID	Understanding Changes in IEC 61511	This course focuses on the specific activities operations and maintenance personnel need to understand and perform to ensure the safety lifecycle as contained in ANSI/ISA S84.00.01-2004 Parts 1-3 (IEC 61511 MOD) is improving the process safety performance at their facility or the facility they are associated with designing / constructing. IEC 61511 mandates a performance-based safety lifecycle approach to risk management. Operations and maintenance staff perform a critical role in the safety lifecycle. In fact, operations and maintenance staff will determine whether or not the actual benefits of safety lifecycle compliance will be achieved or not. Thus, it is imperative that operations and maintenance staff have a good understanding of the specific actions / tasks they need to perform to ensure compliance with IEC 61511 and, more importantly, to improve the process safety performance at their facility or the facility they are associated with designing / constructing.	6 hours					Novice
ISA		IC39M	Management of Alarm Systems	This online course focuses on the key activities of the alarm management lifecycle provided in the ANSI/ISA18.2 standard, Management of Alarm Systems for the Process Industries, and the IEC version, IEC62682. The activities include the alarm philosophy development, alarm rationalization, basic alarm design, advanced alarm techniques, HMI design for alarms, monitoring, assessment, management of change, and audit. You will learn best practices to improve alarm system performance and methods to solve common alarm management problems. You will also learn the metrics to measure success in alarm management and requirements of the ANSI/ISA standard on Management of Alarm Systems.	5 hours	$1,440 - $1,800	Online	Online		Expert
ISA		IC32	Using the ISA/IEC 62443 Standards to Secure Your Control Systems	The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have wreaked so much havoc on corporate information systems. This course provides a detailed look at how the ANSI/ISA99 standards can be used to protect your critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.	2 days	$1,640 - $2000	Live, In-person	Varies		Novice

Using the ISA/IEC 62443 Standards to Secure Your Control Systems	The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have wreaked so much havoc on corporate information systems. This course provides a detailed look at how the ANSI/ISA99 standards can be used to protect your critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.		$1,640 - $2000	Online, Instructor-Assisted	Online	2 months	Novice
Using the ISA/IEC 62443 Standards to Secure Your Control Systems	The move to using open standards such as Ethernet, TCP/IP, and web technologies in supervisory control and data acquisition (SCADA) and process control networks has begun to expose these systems to the same cyberattacks that have wreaked so much havoc on corporate information systems. This course provides a detailed look at how the ANSI/ISA99 standards can be used to protect your critical control systems. It also explores the procedural and technical differences between the security for traditional IT environments and those solutions appropriate for SCADA or plant floor environments.		$1,640 - $2001	Self-Paced	Online		Novice
Assessing the Cybersecurity of New or Existing IACS Systems	The first phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) is to identify and document IACS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. Per ISA 62443-2-1 these assessments need to be performed on both new (i.e. greenfield) and existing (i.e. brownfield) applications. Part of the assessment process involves developing a zone and conduit model of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS). This course will provide students with the information and skills to assess the cybersecurity of a new or existing IACS and to develop a cybersecurity requirements specification that can be used to document the cybersecurity requirements the project.	3 days	$2,200 - $2,700	Live, In-person	Varies		Novice
Assessing the Cybersecurity of New or Existing IACS Systems	The first phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) is to identify and document IACS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. Per ISA 62443-2-1 these assessments need to be performed on both new (i.e. greenfield) and existing (i.e. brownfield) applications. Part of the assessment process involves developing a zone and conduit model of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS). This course will provide students with the information and skills to assess the cybersecurity of a new or existing IACS and to develop a cybersecurity requirements specification that can be used to document the cybersecurity requirements the project.	7 weeks	$2,200 - $2,700	Online, Instructor-Assisted	Online		Novice
Assessing the Cybersecurity of New or Existing IACS Systems	The first phase in the IACS Cybersecurity Lifecycle (defined in ISA 62443-1-1) is to identify and document IACS assets and perform a cybersecurity vulnerability and risk assessment in order to identify and understand the high-risk vulnerabilities that require mitigation. Per ISA 62443-2-1 these assessments need to be performed on both new (i.e. greenfield) and existing (i.e. brownfield) applications. Part of the assessment process involves developing a zone and conduit model of the system, identifying security level targets, and documenting the cybersecurity requirements into a cybersecurity requirements specification (CRS). This course will provide students with the information and skills to assess the cybersecurity of a new or existing IACS and to develop a cybersecurity requirements specification that can be used to document the cybersecurity requirements the project.		$2,000	Self-Paced	Online		Novice
Cybersecurity Design, Implementation & Testing	Focuses on the activities associated with the design and implementation of IACS cybersecurity countermeasures. This involves the selection of appropriate countermeasures based upon their security level capability and the nature of the threats and vulnerabilities identified in the Assess phase. This phase also includes cybersecurity acceptance testing of the integrated solution, in order to validate countermeasures are properly implemented and that the IACS has achieved the target security level. This course will provide students with the information and skills to select and implement cybersecurity countermeasures for a new or existing IACS in order to achieve the target security level assigned to each IACS zone or conduit. Additionally, students will learn how to develop and execute test plans to verify that the cybersecurity of an IACS solution has properly satisfied the objectives in the cybersecurity requirements specification.	4 hours	$2,700	On-Demand, Self-Paced	Online		Intermediate
Cybersecurity Operations & Maintenance	Part of the ISA's Cybersecurity Certificate Program The third phase in the IACS Cybersecurity Lifecycle (defined in ISA/IEC 62443-1-1) focuses on the activities associated with the ongoing operations and maintenance of IACS cybersecurity. This involves network diagnostics and troubleshooting, security monitoring and incident response, and maintenance of cybersecurity countermeasures implemented in the Design & Implementation phase. This phase also includes security management of change, backup and recovery procedures and periodic cybersecurity audits. This course will provide students with the information and skills to detect and troubleshoot potential cybersecurity events as well as the skills to maintain the security level of an operating system throughout its lifecycle despite the challenges of an ever-changing threat environment.	5 hours	$1,600 - $2,000	On-Demand, Self-Paced	Online		Novice
Overview of ISA/IEC 62443 for Product Suppliers	The use of commercial off-the-shelf (COTS) technologies and the increase in internetworking of Industrial Automation and Control Systems (IACS) has exposed IACS to similar vulnerabilities as information systems. The product supplier has a key role to play in the supply chain and the security of an IACS solution. This course provides an overview of how the ISA/IEC 62443 series of standards can be used by the supplier to implement a security development lifecycle, and to develop IACS systems and components that are secure by design and offer security by default. The course also covers how to independently certify that these systems and components comply with the relevant ISA/IEC 62443 standards. By understanding the value of ISA/IEC 62443 standards the product supplier can incorporate these standards, into their business and communicate the standards' value within their organization and to their customers.	3 hours	$650 - $815	On-Demand, Self-Paced	Online		Novice
Certified Automation Professional (CAP) Online Exam Review Course	This self-paced, online course reviews the knowledge and skill areas included on the Certified Automation Professional® (CAP®) certification program examination. The intent is to prepare an automation professional who meets the exam criteria to take the exam. The content is based on the Job Analysis Domains, Tasks, Knowledge Areas, and Skill Areas developed as the basis for the CAP certification exam. This course is the recommended replacement for the discontinued CAP Learning System preparation tool, as it incorporates content similarly included in that tool.	13 weeks	$1,680 - $2,105	On-Demand, Self-Paced	Online		Novice
Certified Automation Professional (CAP) Online Exam Review Course	This self-paced, online course reviews the knowledge and skill areas included on the Certified Automation Professional® (CAP®) certification program examination. The intent is to prepare an automation professional who meets the exam criteria to take the exam. The content is based on the Job Analysis Domains, Tasks, Knowledge Areas, and Skill Areas developed as the basis for the CAP certification exam. This course is the recommended replacement for the discontinued CAP Learning System preparation tool, as it incorporates content similarly included in that tool.	21 hours	$1,680 - $2,100	On-Demand, Self-Paced	Online		Novice
Safety Instrumented Systems: A Life-Cycle Approach	The course focuses on the engineering requirements for the specification, design, analysis, and justification of safety instrumented systems for the process industries. Students will learn how to determine safety integrity levels and evaluate whether proposed or existing systems meet the performance requirements.	8 weeks	$3,100 - $3,830	Online, Instructor-Assisted	Online		Expert
Fire and Gas System Engineering - Performance Based Methods for Process Facilities	Fire and gas detection and suppression system design techniques that are currently in use are often considered to be unsatisfactory due to their nature of being rule of thumb and experience-oriented without any real ability to quantify risk. This has resulted in systems that are either overdesigned or under-designed. Only after the ISA TR 84.00.07, was a comprehensive framework for performance-based fire and gas design established. This course describes the techniques recommended in the technical report, along with hands-on use of the techniques and associated software tools. This course was designed for all audiences from high-level decision makers and users of FGS including a basic understanding of design techniques to a comprehensive case study that involves employing software to develop a complete performance-based design for a sample oil and gas production facility.	3 days	$1,560 - $1,955	Online	Online		Fundamentals
Cybersecurity Practices for Industrial Control Systems	This training will cover standard cybersecurity practices with information specific to industrial control systems (ICS). It highlights the type of information an adversary may view as valuable. The training provides tools to recognize potential weaknesses in daily operations, as well as effective techniques to address those weaknesses.	2 hours	Free	Online	Online		Fundamentals
Differences in Deployments of Industrial Control Systems	Cyber-attacks on critical infrastructure are a growing problem. Every day, there are disclosures about vulnerabilities in computer systems that run critical infrastructures. We have made progress in strengthening the resiliency of our control systems, but some of our most critical systems depend on technology that was not designed to protect our systems against the types of attacks we are seeing today. This course discusses what, where, and how industrial control systems (ICSs) are used and describes some of specific examples of how ICSs work in real-life situations.	1 hour	Free	Online	Online		Fundamentals
Influence of IT Components on Industrial Control Systems (ICS)	If you understand what the components of IT networks do and they communicate, you can better recognize their use in ICS networks. This course covers the elements of a traditional IT network, specific issues that relate to emerging cybersecurity problems, and some of the complexity associated with trying to mitigate those problems.	1 hour	Free	Online	Online		Fundamentals

Common ICS Components	This course covers the common components found in Industrial Control Systems (ICS). It reviews the components found in most ICS.	1 hour	Free	Online	Online		Fundamentals
Cybersecurity Within IT and ICS Domains	A move to integrate the components of Information Technology (IT) and Industrial Control Systems (ICSs) has created security concerns, as interconnections between IT and ICS may increase the vulnerability of the ICS to cyber attacks. Understanding the basic concepts of cybersecurity will provide the necessary foundation to determine the appropriate controls to protect ICS. ICSs are dependent on IT, as contemporary IT is often troubled with cyber vulnerabilities.	1 hour	Free	Online	Online		Fundamentals
ICS Cybersecurity Risk	This course is designed to help you gain a better understanding of cyber risk, how it is defined in the context of ICS security, and the factors that contribute to risk. This will empower you to develop cybersecurity strategies that align directly with the ICS environment. You will also learn how IT-based countermeasures can be customized to accommodate for the uniqueness of ICS architectures.	1 hour	Free	Online	Online		Fundamentals
ICS Cybersecurity Threats	Risk is a function of threat, vulnerability, and consequence. The most complex attribute is threat because it can be intentional or unintentional, natural or man-made. When trying to develop defensive strategies to protect controls systems, it is important to understand the threat landscape in order for appropriate countermeasures or compensating controls to be deployed.	1 hour	Free	Online	Online		Fundamentals
ICS Cybersecurity Vulnerabilities	In this course, we examine some of the current trends in cybersecurity vulnerabilities that contribute directly to cyber risk in Industrial Control Systems (ICSs). The goal is to identify the root causes and their associated countermeasures that can be used to protect control systems.	2 hours	Free	Online	Online		Fundamentals
ICS Cybersecurity Consequences	Consider the potential impact of a successful cyber attack on your ICS. We usually assume that they will be more severe if you are manufacturing a toxic chemical than if you making simple widgets. A cyber attack that results in the release of a toxic chemical and kills 10 people is more significant than a cyber attack that temporarily disables the HVAC in a control – or is it? This course will help you better understand the impacts of cyber based attack can have on an ICS, and provide you with different ways of looking at the potential consequences of three types of events.	1 hour	Free	Online	Online		Fundamentals
Attack Methodologies in IT & ICS	A good defense understands what the offense can do. So, the better you can think like an adversary, the better defenses or security you can set up that are specific to your system. Understanding how hackers attack systems helps you better understand how to defend against cyber attacks.	1 hour	Free	Online	Online		Fundamentals
Mapping IT Defense-In-Depth Security Solutions to ICS - Part I	This training will introduce the defense-in-depth model and cover layers 1 and 2.	1 hour	Free	Online	Online		Fundamentals
Mapping IT Defense-In-Depth Security Solutions to ICS - Part II	In the previous training, Mapping IT Defense-In-Depth Security Solutions to ICS - Part I, we covered Layers 1 and 2 of the defense-in-depth model. In this module, we will pick up at Layer 3 - Network Security, and continue to build on the defense-in-depth strategy introduced in Part I.	1 hour	Free	Online	Online		Fundamentals
Introduction to Control Systems Cybersecurity	This course introduces students to the basics of Industrial Control Systems (ICS) cybersecurity. This includes a comparative analysis of IT and ICS architectures, understanding risk in terms of consequence, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the Control System domain.	1 day	Free	Live	Varies		Fundamentals
Intermediate Cybersecurity for Industrial Control Systems Part 1	This course builds on the concepts learned in the Introduction to ICS Cybersecurity (101) course. This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyber attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks. In addition, this course acts as a prerequisite for the next course, Intermediate Cybersecurity for Industrial Control Systems (202), which offers hands-on application of concepts presented.	1 day	Free	Live	Varies		Fundamentals
Intermediate Cybersecurity for Industrial Control Systems Part 2	This course provides a brief review of Industrial Control Systems security. This includes a comparative analysis of IT and control system architectures, security vulnerabilities, and mitigation strategies unique to the Control System domain. Because this course is hands-on, students will get a deeper understanding of how the various tools work. Accompanying this course is a sample Process Control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the hands-on exercises that will help the students develop Control Systems cybersecurity skills they can apply in their work environment.	1 day	Free	Live	Varies		Fundamentals
ICS Cybersecurity	This course provides an online virtual training based on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber-attacks. In order to understand how to defend IT and OT systems, trainees will learn about common cyber vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of systems will enable trainees to identify mitigation strategies, policies, and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment.	3 days	Free	Online	Online		Fundamentals
ICS Cybersecurity	This is the companion and follow-on course to the 301V. This course provides hands-on training on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber-attacks and includes a Red versus Blue team exercise conducted within an actual Control Systems environment. Attendees will get an instructor-led hands-on experience with opensource operating systems and security tools such as Kali Linux and Security Onion. In addition, the training provides the opportunity to network and collaborate with other colleagues involved in operating and protecting Control System networks.	2 days	Free	Online	Online		Fundamentals
ICS Evaluation	This instructor-led 5-day course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization's Industrial Control Systems (ICS) for the purpose of identifying recommended changes. Specifically, the course will utilize a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture. This course is also intended to increase awareness of how a threat related to the Industrial Control System translates into a threat to business operations, either directly through the ICS or indirectly via network connections. Attendees will come to more fully appreciate that most businesses have numerous support processes and systems controlled by, or otherwise dependent on, an Industrial Control System.	5 days	Free	Live	Idaho Falls, ID		Novice

Cyberstrike Capability		1 day	Free	Live			Advanced
ICS Cybersecurity Landscape for Managers	The purpose of this course is to provide the necessary background and basic understanding of the current Industrial Control System (ICS) cybersecurity landscape for decision makers working in an ICS environment. It includes an overview of the elements of the risk equation and how it applies to the cybersecurity of an ICS. Trainees will be introduced to actual threats, vulnerabilities, and consequences, along with tools they can use to help mitigate the cybersecurity risk to their ICS.		Free	Online	Online		Fundamentals
Cybersecurity and Mobility (Course 1 of 4 Cybersecurity: Developing a Program for Your Business Specialization)	This course is for you if you are interested in transitioning toward a managerial role in cybersecurity and mobility. Through interviews with industry experts in this area, you will be able to analyze innovations powering the rapid spread of information technology and how they present new challenges for protecting data. For example, mobile devices increase convenience but often bypass traditional security measures. After this course, you will be able to describe how the nature of the threat evolves, as culprits employ a burgeoning set of sophisticated tools to take advantage of our growing reliance on networks for critical-data exchange.	14 hours	Free	Online	Online		Fundamentals
Cybersecurity and the Internet of Things (Course 2 of 4 Cybersecurity: Developing a Program for Your Business Specialization)	Welcome! You may have heard about the Internet of Things (IoT). But you may also have wondered about what it is. Or for that matter, what does it mean to you or an organization. This course is for you if you are curious about the most recent trends and activities in the internet capabilities and concerns about programmed devices. There are complexities and areas of necessary awareness when the industrial sector becomes connected to your home. Security policies and practices have not yet caught up to the internet capabilities of some of our most common products. The "connected home", "consumer wearables", or even an employee's HVAC system may cause an unanticipated threat to your business environment. You will explore current security and privacy related concerns in each of these areas. Every module will include readings, videos, case studies, and a quiz to help make sure you understand the material and concepts we talk about. This course offers a place to learn, reflect, and plan for a smart community approach to IoT. Portions of this course may seem extremely technical in nature. That is because the "things" in IoT represents engineering. Try to grasp the concept in that case.	11 hours	Free	Online	Online		Fundamentals
Cybersecurity and the X-Factor (Course 3 of 4 Cybersecurity: Developing a Program for Your Business Specialization)	What is the X-Factor? In Cybersecurity, the X-Factor related to unknown and unpredictable human behavior within and outside of your organization. "No one really knows why humans do what they do", (David K. Reynolds), and because of this organizations can be unprepared for malicious, untrained, or even best intentioned behavior that can cause alarm and sometimes irreparable harm. This course will introduce you to the types of training available to reduce the impact of the X-Factor, evaluate its effectiveness, explore the Security Education, Training and Awareness (SETA) program, and learn why it may fail. The course will conclude with information designed to assist you with some critical components for your business security program. Activities focused on hactivism, cyberinsurance, and ransomware will round out your knowledge base. Your team of instructors has prepared a series of readings, discussions, guest lectures, and quizzes to engage you in this exciting topic.	12 hours	Free	Online	Online		Fundamentals
The Business of Cybersecurity Capstone (Course 4 of 4 Cybersecurity: Developing a Program for Your Business Specialization)	This course intends to make the student familiar with information security management. When you have finished with this course you will know more about: • Governance: including the mission, roles and responsibilities of the InfoSec governance function, and the strategic planning process and InfoSec's role in the organization's strategic planning effort. • You will understand the various types of InfoSec policies and how effective information security policy is created and used. • Risk management and the risk management process • Certain laws and ethical issues impacting information security in the organization. And some common information security management practices such as benchmarking and performance measures.	17 hours	Free	Online	Online		Fundamentals
Safety Instrumented Systems	Safety Instrumented Systems (SIS for short) are used in many process plants where there is a risk of asset damage, environmental release or human fatalities due to the complex processes in these plants that handle large amounts of explosive and/or toxic materials at high temperatures and pressures. In case of failure of any of the loops of a basic process control system (such as a DCS or a PLC/SCADA system) the SIS can take control autonomously and bring the plant or facility to a safe state. This course will help you learn all about these systems in detail.	40 hours	$399 - $499	Online	Online		Fundamentals
HAZOP	Hazard and Operability Study, is a well known hazard analysis tool used for risk assessment and mitigation. It is considered an important part of process safety management and HSE risk assessment of plants and facilities. It is a highly structured and systematic method, to identify all hazards in a process, evaluate the design intention, work out possible deviations & then think of mitigating those which could cause bad consequences. The deviations also include human factors, including non malicious as well as malicious intent.	20 hours	$399 - $499	Online	Online		Advanced
Fieldbus	Fieldbus is an all digital communications technology used in Industrial Automation systems to communicate between instruments in the field. The main protocols that are in use today include FOUNDATION Fieldbus, Profibus PA, HART and Asi. These are all covered in this comprehensive self learning e-course. Learners can get a Certificate of Completion, as well as an electronic badge via Credly, after completing the course and the associated exam.	40 hours	$399 - $499	Online	Online		Novice
Hazardous Area Instrumentation	Hazardous Area Instrumentation is essential to know for all Instrumentation, Automation & Control or Electrical engineers who design, operate, build and maintain equipment used in hazardous areas such as those found in Oil & Gas installations, chemical plants, coal handling plants and so on, where the risk of fire and explosion is very high.	16 hours	$399 - $499	Online	Online		Novice
Gas Monitors	Gas Monitors (also referred to as Gas Detectors) are used to detect and measure explosive gases & vapors, toxic gases and Oxygen. These are a very important part of Instrumentation of any plant or facility. These can be portable as well of a fixed type and very often are combined with other systems, such as Fire Alarm and suppression systems. This easy e-learning course will help you understand everything about gas detection in a few hours.	10 hours	$199 - $299	Online	Online		Novice
RFID (Radio Frequency Identification)	As a technical professional working in any of these industries, it is essential to understand how this new technology works and how it can benefit organizations by increasing productivity, reducing pilferage, increasing throughput and efficiency all around. However until now, there was no single resource that one could refer to, that explained this new technology in an easy to understand manner, without complicated math and physics, or partial differential equations (ugh!) or other such complex stuff.	8 hours	$199 - $299	Online	Online		Novice
AC Variable Frequency Drives	AC Variable Frequency drives have become very popular in recent years and have become an integral part of implementing Industrial Automation systems. This easy e-learning course will help you understand everything about VFDs in a few hours.	10 hours	$199 - $299	Online	Online		Novice
Safe Chemical Warehousing	The importance of safety in today's chemical storage facilities cannot be overstated. These facilities store everyday, hundreds or even thousands of tons of chemicals and are located in various areas, such as industrial manufacturing plants, logistics parks, shipping yards, ports and even airports. If you have been involved in the business of chemicals (including hydrocarbons, specialty chemicals, pesticides, agrochemicals, fertilizers,etc), you must have realized that they need to be handled safely. This is not only to avoid the possibility of damage of goods, but also damage to the facilities, environment and even the general public at large.	20 hours	$299 - $399	Online	Online		Novice
Industrial Cybersecurity	Most modern plants and facilities today use some kind of DCS, PLC, SCADA or SIS to monitor, control and safely shutdown the process. However most of these Industrial Automation systems are not secure. This is why today ICS Security (also referred to as Industrial Cybersecurity) has become very important. In case of business and IT systems, a cybersecurity breach can result in monetary losses or in loss of proprietary data. However in case of an Industrial cybersecurity incident, there can be a physical disaster since these cyber-physical systems control large plants and facilities that often time process huge amounts of hazardous, explosive and/or toxic materials.	40 hours	$499 - $695	Online	Online		Fundamentals

Confined Space Safety	Confined Space Safety Training & Certification- compliant with OSHA guidelinesA Lack Of Knowledge Can Cost You Your Job, Your Money, Your Business... Even Your Life...Shocking fact! Every year hundreds of employees die every year from ignorance about working in confined spaces. The employees lose their life and the employers lose their best workers	4 hours	$99 - $199	Online	Online		Fundamentals
Hazardous Area Classification	These areas (also known as "Classified Locations") are those parts of a plant or facility where the risk of an explosion or fire is higher than normal, due to the kind of material stored, handled or processed in that area. This includes commonly known places such as gasoline storage tank farms and terminals, oil refineries, gas processing plants, chemical plants, warehouses that store hazardous chemicals and even plants that process large amounts of dusty materials such as sugar, grains and so on.	12 hours	$399 - $499	Online	Online		Fundamentals
Industrial Toxicology	Toxicology is the study of toxins, in other words, poisons. Many industrial processes use materials that are either toxic by themselves or create materials that may be toxic (poisonous). These toxins may affect humans, plants, animals and the environment.This course is in the popular Abhisam XPRTU format. This means that you will see a mix of text, animations, videos and pictures, real life examples and exercises that help you gain a deep understanding of the subject.	10 hours	$299 - $399	Online	Online		Fundamentals
ICS Cybersecurity for Managers	This course was developed and is taught by two highly experienced professionals: a former CISO of an oil and gas company, and the vice-president of industrial cybersecurity for an engineering and process safety services firm. The course is a "Reader's Digest" of what the instructors have learned over the last decade regarding effective management and implementation of an ICS/OT cybersecurity program. Throughout the course, they share practical advice and illuminating anecdotes about their experiences working with both large and small companies across a wide range of industries. You will leave with a set of techniques, tools, and templates to more confidently lead your company's ICS/OT cybersecurity program.		$1,195	Live			Fundamentals
ICS Cybersecurity In-Depth	The course concepts and learning objectives are primarily driven by the focus on hands-on labs. The in-classroom lab setup was developed to simulate a real-world environment where a controller is monitoring/controlling devices deployed in the field along with a field-mounted touchscreen Human Machine Interface (HMI) available for local personnel to make needed process changes. Utilizing operator workstations in a remotely located control center, system operators use a SCADA system to monitor and control the field equipment. Representative of a real ICS environment, the classroom setup includes a connection to the enterprise, allowing for data transfer (i.e., Historian), remote access, and other typical corporate functions.	5 days		Live Online	Anywhere		Novice
ICS/SCADA Security Essentials	Provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.	5 days	$7,020	On-Demand	Anywhere	4 months	Novice
Essentials for NERC Critical Infrastructure Protection	Empowers students with knowledge of the what and the how of the version 5/6/7 standards. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6/7 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.	5 days	$6,090	On-Demand	Anywhere	4 months	Intermediate
ICS Active Defense and Incident Response	ICS Active Defense and Incident Response will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. This process of monitoring, responding to, and learning from threats internal to the network is known as active defense. An active defense is the approach needed to counter advanced adversaries targeting ICS, as has been seen with malware such as Stuxnet, Havex, and BlackEnergy2. Students can expect to come out of this course with the ability to deconstruct targeted ICS attacks and fight these adversaries and others. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations. The strategy and technical skills presented in this course serve as a basis for ICS organizations looking to show that defense is do-able.	5 days	$7,020	On-Demand	Anywhere	4 months	Intermediate
Assessing and Exploiting Control Systems	This is not your traditional SCADA/ICS/IoT security course! How many courses send you home with your own PLC and a set of hardware/RF hacking tools?!? This course teaches hands-on penetration testing techniques used to test individual components of a control system, including embedded electronic field devices, network protocols, RF communications, Human Machine Interfaces (HMIs), and various forms of master servers and their ICS applications. Skills you will learn in this course will apply directly to systems such as the Smart Grid, PLCs, RTUs, smart meters, building management, manufacturing, Home Area Networks (HAN), smart appliances, SCADA, substation automation, and synchrophasors. This course is structured around the formal penetration testing methodology created by UtiliSec for the United States Department of Energy. Using this methodology and Control Things Pentest Platform (previously SamuraiSTFU), an open source Linux distribution for pentesting energy sector systems and other critical infrastructure, we will perform hands-on penetration testing tasks on user interfaces (on master servers and field device maintenance interfaces), control system protocols (modbus, DNP3, IEC 60870-5-104), RF communications (433MHz, 869MHz, 915MHz), and embedded circuit attacks (memory dumping, bus snooping, JTAG, and firmware analysis).	5 days	$7,270	Live			Advanced
Critical Infrastructure and Control System Cybersecurity	This course is an intermediate to advanced course covering control system cybersecurity vulnerabilities, threats and mitigating controls. This course will provide hands-on analysis of control system environments allowing students to understand the environmental, operational and economic impacts of attacks like Stuxnet and supporting mitigating controls.	5 days		Live			Intermediate
Certified SCADA Security Architect (CSSA)	The CSSA determines if a candidate possess adequate knowledge to properly secure a SCADA system. It is designed to be relevant for power transmission, oil and gas and water treatment industries. The CSSA certification provides professionals with an objective measure of competence as well as a recognizable standard of achievement. The CSSA credential is ideal for industrial network administrators and their managers, as well as IT professionals and their managers. The CSSA certification encompasses the following domains: · SCADA security policy development · SCADA security standards and best practices · Access Control · SCADA protocol security issues · Securing field communications · User authentication and authorization · Detecting cyber attacks on SCADA systems · Vulnerability assessment		$34/month - $339/voucher - $499/exam	Online courses, Live tests	Anywhere		Advanced
ICS/SCADA Cyber Range: Lights Out Capture the Flag	Put on your white hat and try to prevent a major disaster from happening by solving 10 ICS/SCADA pentesting challenges.	9 hours	$34/month	On-Demand	Anywhere		Advanced
SCADA Security Frameworks	This course will begin your reintroduction to SCADA security frameworks, covering common threats to SCADA, relevant security standards and bodies, developing SCADA security polices and more.	66 minutes	$34/month	On-Demand	Anywhere		Novice
SCADA Security Assessment	Review your understanding of SCADA security assessment with this course covering SCADA security objectives, security assessment programs and more.	44 minutes	$34/month	On-Demand	Anywhere		Novice
SCADA Device Identification and Analysis	Make sure you know what you need to know with this course on SCADA device identification and analysis.	43 minutes	$34/month	On-Demand	Anywhere		Intermediate

SCADA Vulnerabilities	Explore SCADA vulnerabilities with this course covering common vulnerabilities, vulnerability scanning, server OS testing and more.	26 minutes	$34/month	On-Demand	Anywhere		Intermediate
Pentesting SCADA Services and Protocols	Review what it takes to attack standard services, server OS, ICS protocols and more with this course on pentesting SCADA services and protocols.	24 minutes	$34/month	On-Demand	Anywhere		Intermediate
SCADA Access Controls	In this course, you'll look at the importance of SCADA access controls. Review physical safety, access control models and more.	31 minutes	$34/month	On-Demand	Anywhere		Novice
Remote Access and Field Site Security	Re-familiarize yourself with the challenges of remote access technologies, field site firewalls and more.	36 minutes	$34/month	On-Demand	Anywhere		Novice
SCADA Network Security	In this course, you'll refresh your knowledge of SCADA network security through secure network design, firewalls and logical security zones.	39 minutes	$34/month	On-Demand	Anywhere		Advanced
SCADA Intrusion Detection and Incident Response	Get to grips with what you need to know for SCADA intrusion detection and incident response.	61 minutes	$34/month	On-Demand	Anywhere		Intermediate
SCADA Preventative Controls	Brush up on what you need to prevent or mitigate disasters with this course on SCADA preventative controls.	46 minutes	$34/month	On-Demand	Anywhere		Novice
Advanced Insider Threat Mitigation	The purpose of this course is to highlight approaches and techniques that mitigate risks posed by insider threats.						Fundamentals
ARCyber	This course is intended for U.S. military and/or Department of Defense personnel assigned to conduct cyber vulnerability evaluations of DOD critical infrastructure.	10 days	Free				Advanced
Consequence-driven Cyber-informed Engineering (CCE)	Consequence-driven Cyber-informed Engineering (CCE) is a new methodology focused on securing the nation's critical infrastructure systems. Developed at Idaho National Laboratory, CCE starts with the assumption that if a critical infrastructure system is targeted by a skilled and determined adversary, the targeted network can and will be penetrated. This think like the adversary approach provides critical infrastructure owners, operators, vendors and manufacturers with a disciplined methodology to: Evaluate complex systems; Determine what must be fully safeguarded; Apply proven engineering strategies to isolate and protect an industry's most critical assets.						Advanced
CCE ACCElerate	Course will provide participants with a fundamental knowledge of the CCE methodology focused on securing the nation's critical infrastructure systems. Participants should be critical infrastructure owners, operators, vendors, and manufacturers.	16 hours		In Person			Fundamentals
Cyber Fallout	The purpose of this course is to familiarize participants with key technologies found in a nuclear facility, identify skills needed to assess cyber risk and vulnerabilities. Participants will leave the workshop with a greater understanding of the digital footprint typical of nuclear facilities, their vulnerabilities, how to assess those vulnerabilities, and typical controls used for mitigations.						Fundamentals
Cybersecurity Fundamentals	Is a high level introductory course designed to expose participants to the challenges and frameworks used in implementing and sustaining a cyber security program at a nuclear and/or radiological facility. The course uses the National Institute of Standards and Technology (NIST) cyber security framework as the course structure for conveying the core concepts and components of a cyber security program. This includes, identifying sources of risk, protection of digital systems, detection concepts should protection fail, response to detection points, and recovering the system back to conditions before a cyber event.						Novice
Cyberstrike	The CyberStrike training is designed to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting industrial control systems. This training offers participants a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine. During this training participants are guided through a series of exercises that challenges learners to defend against a cyberattack on the equipment they routinely encounter within their industrial environment.						Advanced
DHS Basic Incident Responder Training (BIRT)	This two-day course will provide participants with a baseline of knowledge and skills regarding processes, procedures, resources, and tools used for incident response (IR) functions. It is intended to maintain a consistent quality for engagements in an environment where the make-up of the engagement team involves a wide variety of capabilities and could include personnel from DHS, other Federal agencies, public, and private organizations (including any surge capacity).	2 days					Intermediate
IAEA Computer Security for Nuclear Facilities International Training Course	The purpose of this 2 week training is to educate participants regarding computer security related issues within nuclear security of nuclear facilities. To familiarize participants with key technologies found in a nuclear facility, identify skills needed to assess cyber risk and vulnerabilities. Participants will leave the workshop with a greater understanding of the digital footprint typical of nuclear facilities, their vulnerabilities, how to assess those vulnerabilities, and typical controls used for mitigations.	10 days					Fundamentals
Managing Cyber Risks	Is an introductory course that raises awareness of cyber risks to operational technologies commonly used at nuclear facilities. The course identifies how digital components are increasingly becoming the backbone of nuclear security and nonproliferation tools and how this integration has changed risk profiles. The course is designed to introduce these risks as well as raise awareness about core risk mitigation concepts for cyber security.						Fundamentals
Maritime ICS Cybersecurity Fundamentals	This week-long training will provide a baseline of knowledge and skills specific to critical infrastructure elements, including industrial control systems (ICSs) and their cyber components on maritime platforms. Specifically, this training covers maritime industry platforms, systems-of-systems, underlying information technology (IT) and ICS infrastructures, and feedback control system concepts. Most importantly, it will highlight the cyber interconnectivity of these systems to show the interdependencies of each device on another.						Fundamentals
Advanced Radiation Detection Training (CST)	ARDT training is for the National Guard Bureau (NGB) Civil Support Team program, the training provides hands on detection of sources, DOE triage submission, responder math, and contamiantion avoidance training. The highlight of the course is a post RDD detonation entry into a contamination fall out plume.						Advanced
Advanced Radiological Detection Training (ARDT) WMD-Civil Support Team (93rd & 91st CST)	This training provides members of the US WMD-CST advanced concepts for use in response to an intentional or unintentional release of nuclear or radiological materials. The training enables members of the WMD-CST teams to identify hazards, assess consequences, and advise on response measures through the development, testing and implementation of tactics, techniques and procedures.						Advanced
DOD/DOJ Radiography Techniques Training	This training, conducted by DOE NNSA through INL, provides high-fidelity weapons of mass destruction training for the Render Safe community of both the DOD and DOJ. The National Laboratories provide special technical support by providing technical support/training for training and readiness exercises, both at INL and offsite locations.						Advanced
DOE NNSA Stabilization Training	This training, conducted by DOE NNSA through INL, and other National Laboratories provided detailed information on nuclear physics, radiation safety, radiological dispersal devices (RDD) science, radiation survey techniques. This is accomplished through both classroom instruction, and practical exercises.						Advanced
Naval Explosive Ordnance Disposal (NEOD) Team Training	This training, conducted by DOE NNSA through INL, provides special expertise supporting US Navy Explosive Ordnance Disposal units in the areas of radiography, and radiological and nuclear hazards and assessments.						Advanced
Nuclear Infrastructure Assessment and Disablement (NIAD) Training	This is a 10-day training course comprised of classroom, facility tours, and field practicals that provides the students with an understanding of basic and advanced nuclear fuel cycle processes.	10 days					Novice
Radiological Hazards and Operations Course (RHOC)	This is a 10-day training course and field exercise where DOD (primarily US Army) personnel are trained to: respond to accidents and incidents involving radiation or radioactive materials, conduct radioactive source recovery operations, and provide radiological site assessments of areas suspected to be contaminated with radioactive material.	10 days					Advanced

Explosive Breaching/Blast Effects	Instruction on explosive and mechanical breaching calculations, techniques and execution. Predicting explosive effects with software models.	4 hours		In Person			Expert
Army 2A	The Army 2A course teaches Army cyber assessment teams the fundamental thru intermediate levels of how to conduct an cyber assessment on ICS networks and systems.			Web Based			Advanced
Army 2B	Advanced ICS cybersecurity assessors training.			Web Based			Advanced
Industrial Cybersecurity Awareness Training	Helps your non-IT/OT specialists to increase their awareness of the current industrial cybersecurity issues by learning about IT/OT differences and similarities, general cyber security basics and industrial cybersecurity specifics. Raises awareness for your IT/OT specialists of current industrial cybersecurity trends; both attacks and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.	1 day					Fundamentals
Industrial Cybersecurity Awareness Training for Executives and Managers	Helps executives and managers develop their awareness of current industrial cybersecurity issues and recent incidents, identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT networks, and understand how the evolution of the Internet of Things can impact ICS security.	3 hours					Fundamentals
Advanced Industrial Cybersecurity in Practice	Raises awareness for your IT/OT specialists of current industrial cybersecurity trends; both attacks and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.	2 days					Novice
Digital Forensics and Incident Response in ICS	Enables IT/OT security professionals to conduct successful forensic investigations in industrial environments and to provide expert analysis and recommendations.	5 days					Intermediate
Digital Forensics and Incident Response in ICS with in-depth practice	Enables IT/OT security professionals to conduct successful forensic investigations in industrial environments and to provide expert analysis and recommendations.	10 days					Intermediate
IoT Vulnerability Research and Exploitation	Raises awareness for your IT/OT specialists of current industrial cybersecurity trends; both attacks and protection techniques. Your staff members will learn to identify the main types of ICS vulnerabilities, clarify the key differences between typical ICS and pure IT malware, and understand how the on-going evolution of the Internet of Things can impact ICS security.	3 days					Novice
Industrial Cyber-Safety Games	On-site and online interactive training modules and cyber-safety games conducted at all levels of technical expertise. These games are always modified for the appropriates levels of technical expertise ranging from executives and management to IT/OT personnel, to any employees who interact with industrial automation systems – on production lines, in the control room or in the back office.	2 hours					Intermediate
Understanding, Assessing and Securing Industrial Control Systems	This course is focused entirely on securing or "blue teaming" the industrial control system (ICS) architecture, and will include technical deep dives, optional demonstrations, and other relevant content that will be used to reinforce the selection and implementation of security controls relating specifically to ICS. The initial online version of this course will NOT include any lab exercises. The lab component of the course will be offered (in the future) as an optional purchase.	40 - 120 hours	$3,000	Online	Online		Intermediate
Tempcon DDC Fundamentals	This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical and practical working knowledge of the operations of DDC control systems.	36 hours	$700				Novice
Metasys Extended Architecture for Building Operators	This three-day course teaches building personnel how to make the most effective and efficient use of the features of a Metasys® system extended architecture building management system. This course is for building personnel who have new installations of Metasys® system extended architecture using NAEs or NIEs or for those who have migrated from their existing Metasys® system.	24 hours	$1,520				Fundamentals
Metasys Extended Architecture for Engineers	This course teaches building personnel how to make the most effective and efficient use of the features of a Metasys® system extended architecture building management system. This course contains additional topics not covered in the Metasys® system extended architecture for Building Operators course.	16 hours	$1,820				Novice
Introduction to Metasys® N2 Controllers	Introduction to the hardware, software, and tool components of the Metasys® N2 family of controllers. Learn how the hardware interconnects, the protocol used for communication, and the software and hardware tools used to operate and maintain N2 ASC and DX-9100 devices. ASC controllers include VAV, VMA, UNT, and AHU.	28 hours	$2,250				Intermediate

Metasys FEC Operation/Troubleshooting	Designed as a beginners course for people working with Field Equipment Controllers (FECs), this course shows students how to connect to FECs and how to download and test existing control programs. It also covers calibration of input sensors and setup and verification of inputs and outputs. This course is designed for building personnel who want to better understand field controller operation, commissioning and troubleshooting.	24 hours	$1,800				Intermediate
Metasys System Extended Architecture Hardware and Troubleshooting	This hands-on course provides experienced Metasys® users with valuable diagnostic and troubleshooting skills on system hardware. Discussions and exercises cover the full range of Metasys® Network products, with an emphasis on communication solutions and other commonly experienced problems.	16 hours	$1,800				Intermediate
Metasys FEC Custom Programming	Students will learn how to create and test customized control strategies for FEC controllers in this three-day course. The course is designed for experienced building personnel who want to expand their knowledge of HVAC Control Systems and Johnson Controls FEC devices.	32 hours	$1,520				Advanced
Metasys FEC Systems Engineering	In this advanced Field Equipment Controller (FECs) programming class, students will learn how to write and test programs for the (FECs). They will use the software simulation tool to verify that the programs satisfy the sequence of operations. The course is designed for experienced personnel who want to become proficient in writing or revising programs for Johnson Controls FEC devices. Although not a prerequisite, it is highly recommended that students are familiar of the topics found in course	24 hours	$1,520				Expert
Metasys System Extended Architecture Engineering and Setup	Students will learn how to set up and manage the Network Automation Engine (NAE) database and to use the power of the System Configuration Tool to generate an NAE database from existing ASC controller programming.	36 hours	$2,250				Advanced
Metasys System Extended Architecture Advanced Engineering	Experienced personnel will learn how to write advanced programs for facility-wide or specific mechanical control applications using the System Configuration Tool (SCT). Students will build, modify and troubleshoot routines they create.	24 hours	$1,800				Advanced
Graphics Generation Tool	This course teaches students how to create and modify the custom graphics used to both monitor and actively change building parameters and settings in a Metasys® automation system. It is a three-day online internet course which combines active instructor facilitation with student practice sessions with the facilitator available for questions. This course is for individuals interested in creating and editing Graphics+Metasys® graphic files using Graphics Generation Tool (GGT) software.	24 hours	$1,200				Expert
Tempcon DDC Fundamentals	This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical and practical working knowledge of the operations of DDC control systems.	36 hours	$2,250				Novice
Field Tech Basic	There are many different skill sets in the life of a field technician - engineering, IT infrastructure, technical support, and computer programming to name a few. Field Tech - Basic training will prepare field technicians to confidently install, commission, troubleshoot, and edit a WebCTRL system utilizing EIKON, SiteBuilder, ViewBuilder, and WebCTRL. Learners will become familiar with ISA submittal control drawings and the mechanical equipment these drawings represent. Hands on tasks include hardware, networks, and software with an emphasis on real life scenarios with the latest tools available.	16 hours	$1,000				Intermediate
WEBCTL	This course is a great place to start your WebCTRL journey! If you have little or no experience with the Automated Logic WebCTRL system or you've never attended a BASU course, this course is for you. From this course, you will be able to work with the WebCTRL user interface, create operators and privileges, develop schedules, troubleshoot with alarms and trends, and document with WebCTRL's report features. Higher end topics are also included.	24 hours	$1,500				Novice
EIKON	Learn the basics of EIKON programming. Learners who successfully complete this course will be able to identify the different types of microblocks, read a sequence of operations and translate to a program, simulate a program to find errors, and define microblock properties.	16 hours	$1,000				Novice
ViewBuilder - Basic	This course introduces Automated Logic-supplied area and equipment graphics. A complete ViewBuilder overview is covered, as well as its tools, controls, images, and available symbols. Custom topics include the use of conditional expressions and programming floorplans. The learner will be able to successfully develop basic ViewBuilder graphics and provide common editing techniques to existing equipment and area graphics.	16 hours	$1,000				Novice
Networking - Basic	This course covers setup and troubleshooting techniques affiliated with basic Automated Logic networks. In addition, learners will build source trees, define and identify the fundamentals of IP, ARC156, and MS/TP networks, and how these concepts allow devices to communicate. Learners will also learn the basics of Wireshark captures, clippings, and BACnet Discovery. Upon successful completion of this course, learners will be able to properly set up and troubleshoot basic Automated Logic networks, including the use of Wireshark captures to capture IP traffic at the server, IP and ARC156 traffic at devices.	16 hours	$1,000				Novice
Commissioning - Intermediate	This course is designed to challenge the field technician with all aspects of a WebCTRL system. Upon completion of this course, the learner will be able to install and commission a WebCTRL system, provide functional testing of a control program, and apply the most advanced techniques of troubleshooting. The learner will also be responsible for turning in complete check out reports, installing add-ons, and correcting an entire system of common errors, including some obscure "gotchas," using all the skills the learner acquired in WebCTRL, Eikon, ViewBuilder, SiteBuilder, and EquipmentBuilder.	32 hours	$2,000				Intermediate
EIKON - Intermediate	Whether a Field Technician or Design Engineer, learners will expand on knowledge from the EIKON - Basic course to learn how to create complex control programs and logic symbols. The learners will be able to identify programming as it is implemented within a complete system. The learners will also be able to utilize naming standards to create a library for quickly placing previously developed logic into new systems, thus making programming more efficient. Building a properties page, simulating a control program, major customization to EquipmentBuilder programs are among several other intermediate EIKON features offered in this course.	24 hours	$1,500				Intermediate

ViewBuilder - Intermediate	This course allows learners to create equipment graphics from a schematic drawing and technician pages. As an example, learners will be tasked to create one graphic for different types of similar equipment with the idea of creating a master graphic for all VAVs to shorten engineering time. In addition, learners will create a standard template for their company. Upon successful completion of this course, learners will be able to identify, define, and/or apply advanced conditional expressions, WebCTRL paths for system/equipment linking, complete customization of equipment graphics including HTML control, external links, document links, email links, and custom images and symbols for WebCTRL graphics.	24 hours	$1,500				Intermediate
Networking - Intermediate	As part of successful course completion, learners will set up complex ALC networks, troubleshoot networks, and create a secure WebCTRL site. Learners will focus on troubleshooting a WebCTRL system by reading a Wireshark capture. This course is designed for individuals who need to design complex network systems as well as troubleshoot networks with Wireshark.	24 hours	$1,500				Intermediate
Third Party Integration BACnet	BACnet protocol has become the standard protocol within the Building Management Industry. Today, you will be hard pressed to not find BACnet in Building Automated System. In this course a learner will not only learn how to seamlessly integrate third-party BACnet controls into a WebCTRL system, but also understand the theory behind the BACnet protocol. Learners will utilize EIKON, Networking, and ViewBuilder skills to read and write BACnet objects while following a sequence of operation to incorporate them into a WebCTRL system without stressing the network. A successful integration is never complete without commissioning the programming, graphic, and network; Automated Logic Technicians and Engineers will be equipped with tips and tricks to streamline integrating to multiple pieces of equipment and fine tune their BACnet integration to achieve a healthy WebCTRL system, all with emphasis on efficiency.	24 hours	$1,500				Intermediate
Third Party Integration Modbus	Modbus protocol has been the protocol of industrial environment. Today, Modbus can be found in many industrial controls from energy metering to variable frequency drives. In this course a learner will not only seamlessly integrate third-party Modbus controls into a WebCTRL system, but also understand the theory behind the Modbus protocol. Learners will utilize EIKON, Networking, and ViewBuilder skills to read and write from/to Modbus registers while following a sequence of operation to incorporate them into a WebCTRL system without stressing the network. A successful integration is never complete without commissioning the programming, graphic, and network; Automated Logic Technicians and Engineers will be equipped with tips and tricks to streamline integrating to multiple pieces of equipment and fine tune their Modbus integration to achieve a healthy WebCTRL system, all with emphasis on efficiency.	24 hours	$1,500				Intermediate
Design Engineering - Basic	The foundation of every project starts here. This Design Engineering course will introduce the basic fundamentals of creating a complete WebCTRL system package to a field technician for installation. Learners will be challenged by completing a WebCTRL system throughout the entire project life cycle. The project life cycle will include the project scope, review of hardware, a control submittal developed with Engineering Design Suite, and creating a WebCTRL system database. This course strongly encourages the use of standards, the creation of libraries, and the optimal use of an engineer's time. With these skills the objective of the Design Engineer becomes clear: deliver on time, under budget, and mistake free. This course is for Automated Logic branch and independent field office personnel only.	24 hours	$1,500				Novice
Engineering Design Suite	The Microsoft Visio® EDS add-on is a tool that allows you to streamline engineering tasks and the submittal process to make drawings for installing and commissioning, create project reports, and control your revisions. The add-on includes built-in components with data sheets, engineering calculators and conversions, Cv calculations for water and steam, a building riser manager, a valve schedule creator, and a searchable library in which you can add items. Data can be output to Microsoft Excel® in standalone spreadsheets or embedded in the Visio® EDS drawings. It provides automated creation of sequence of operation and your final drawing package.	16 hours	$1,000				Intermediate
Tempcon DDC Fundamentals	This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical and practical working knowledge of the operations of DDC control systems.	36 hours	$550				Novice
Introduction to the Tracer SC System	This course introduces you to the Tracer Synchrony interface and common tasks performed using it.	1.5 hours	$0				Fundamentals
Tracer Ensemble for Operators	This course provides a good introduction to many of the features of Tracer Ensemble as you walk through various real-life scenarios commonly encountered by a Tracer Ensemble building operator.	1 hour	$0				Fundamentals
Tracer ES Operations-Curriculum for Operators	This curriculum will walk the student through common tasks they would perform while using their Tracer ES building management system.	1.5 hours	$0				Novice
Introduction to Computer Networking on Tracer Summit	This course provides the student the knowledge and skills needed to install a simple building automation system on a customer's existing network.	2 hours	$0				Novice
Introduction to LonTalk	This course explains what LonTalk is, identifies the existing network management tools Trane uses, and provides a basic understanding of technology and terminology. This course does not include use of third party software to extract the xif or any other concepts not covered in the learning objectives.	2 hours	$0				Novice
Tracer Ensemble Operation	Tracer Ensemble Operation is specifically designed for building operators and administrators to become more efficient with their Tracer Ensemble software which is a Web-enabled service and monitoring tool for multiple building facilities. Tracer Ensemble allows building operators and administrators access to Tracer Ensemble from the local network or the Internet to monitor and control their building system. Students will have the opportunity to work with the Tracer Ensemble software to become more familiar with common tasks.	20 hours	$1,320				Intermediate
Tracer Synchrony Operation	In the Tracer Synchrony Operation course, students learn to operate and modify an installed Tracer SC+ system using the Synchrony interface. This highly interactive course includes presentations, demonstrations and hands-on workshops where students practice using the software applications integral to a Tracer SC+ building management system.	20 hours	$1,320				Intermediate
Tracer Summit System Operation	In this course students will learn to perform common and advanced operations with their installed Tracer Summit building management system. This highly interactive basic course includes presentations and hands-on workshops where students practice using the common applications of a Tracer Summit building management system and learn how to monitor and control building mechanical systems.	20 hours	$1,550				Intermediate

Tracer Summit Controls Service		36 hours	$1,980				
Tracer Synchrony Advanced Operation	The Tracer Synchrony Advanced Operation course builds on the knowledge and skills learned in the Tracer SC/Synchrony Operation course. This course will enable learners to expand their skillset to complete a variety of advanced operations, control strategies and energy saving methods to get the most value out of their Tracer SC+ building control system.	24 hours	$1,320				Advanced
Tempcon DDC Fundamentals	This course is designed to introduce HVAC personnel to the concepts of computer Direct Digital Control systems. Individuals who attend this seminar should have a good background in HVAC systems and conventional (pneumatic and/or electronic) control principles. Attendees to this seminar can expect to gain a good theoretical and practical working knowledge of the operations of DDC control systems.	36 hours	$550				Novice
Introduction to Desigo CC	This web-based training course provides an introduction to the Desigo CC Management Station.	0.5 hours	$0	Web-Based			Fundamentals
Desigo CC Workstation I	Learn how to monitor and control your Desigo CC Management Station through hands-on guided exercises and discussions. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.	24 hours	$1,950				Novice
Desigo CC Workstation II	Building on Desigo CC Workstation I, you will learn how to build and modify system objects. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.	28 hours	$2,195				Intermediate
Terminal Equipment Controller (TEC) Basics	This web-based training course provides basic information about TECs.	0.5 hours	$0	Web-Based			Fundamentals
PXC-Modular Field Panel and TX-I/O	This web-based training course explains the operation and features of the PXCModular Field Panel.	0.5 hours	$0	Web-Based			Novice
Field Panel and FLN Operations	Learn to monitor, control and configure building automation systems locally from field panels and FLN devices using Datamate Advanced. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.	28 hours	$1,895				Intermediate
Desigo CC Master Operator	Configure and modify applications within Desigo CC to increase your efficiency in monitoring and controlling building systems	24 hours	$1,950				Advanced
Introduction to Control Programming	This web-based training course covers the flow and functionality of creating, editing and saving a building's control program.	0.5 hours	$0				Intermediate
PPCL Programming I	Learn to develop and modify a PPCL program. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.	28 hours	$2,195				Intermediate
PPCL Syntax Review	This web-based course provides information on PPCL syntax and structure.	12 hours	$975				Novice
PPCL Programming II	Learn to build and optimize PPCL programs to improve building efficiency and incorporate staging and rotating of equipment. A scenario-based skills assessment at the end of the course allows you to put into practice the knowledge you have learned.	28 hours	$2,195				Intermediate
PPCL Master Programmer	This course provides complex PPCL programming scenarios for you to read, troubleshoot and correct. Upon successful completion of the training path, students will earn Master Programmer status.	24 hours	$1,950				Advanced

Harmony Rack I/O with Composer	Students will learn about the features of the Symphony/Infi90 Open control system and the Harmony Control Unit hardware components. Using a simple process control loop model as a base project, students will utilize Composer software tools to create a process control strategy. “Hands-on” exercises provide the opportunity for monitoring, tuning, and diagnostics of the Harmony Control Unit with Composer software.	40 hours	$3,300				Intermediate
Composer Engineering Software Tools	In this course, students will learn a complete methodology for Symphonyâ/Infi90 Openâ control system documentation and controller programming. Using a simple process control loop model as a base project the student will utilize the Composer software to create a process control strategy and documentation. This course will also discuss the monitoring, tuning, and diagnostic capabilities of the Composer software. A discussion of the overall. Client/Server networking architecture and global database generation will be discussed. Additionally, this course builds upon the knowledge acquired in M101, M111 or M201, and prepares the student for the Human System Interface courses.	40 hours	$3,300				Advanced
Harmony Configuration Strategies	This is an advanced course in which students will build upon their previous control system programming knowledge and implement control strategies to solve process control problems.	40 hours	$3,300				Expert
SEL-3530 RTAC	The APP 3530 course is designed to be highly interactive and activity-based. During APP 3530, in groups of two, you will configure a realistic communications scheme using the SEL-3530 RTAC. Each section of this course will guide you, step by step, through configuring this communications scheme.	24 hours	$1,425				Advanced
SEL-2032	Students will learn to use the SEL-2032 Communications Processor to design, create, and implement a state-of-the-art substation integration and automation system. Detailed hands-on examples will show the ease with which you can apply the communications processor to both SEL relays and non-SEL IEDs. Students will explore use of the communications processor with DNP3 Level 2, Modbus, and the SEL-2701 Ethernet Processor. Multitier applications of the communications processor are also addressed. Students (in groups of two) will gain hands-on experience in communicating, setting, and reporting functions directly with an SEL communications processor.	24 hours	$1,425				Advanced
APP-351 or other relays	APP 351 provides comprehensive application training for the SEL-351 Protection System, an extremely flexible protective relay used by utilities worldwide, in multiple applications. Working in groups of two, students gain hands-on experience in communicating, setting, metering, monitoring, retrieving event reports, and performing control functions by working directly with the SEL-351S Relay.	16 hours	$950				Advanced
Power Meter Training Programs	The two-day seminar offers practical training on EIG meters for customers, potential customers, and representatives. The training introduces you to the Nexus® and Shark® lines of power meters and monitors, with hands on setup and troubleshooting as an introduction to CommunicatorPQA™ advanced power monitoring and analysis software.	16 hours	$0				Novice
Hardware Installation and Troubleshooting		32 hours	$3,334				Intermediate
PME Operation Bundle		32 hours	$3,576				Expert
PME Admin and Maintenance		32 hours	$3,334				Novice
GENESIS32 Standard or like	The GENESIS32 Standard course is a 5-day, hands-on, instructor led class designed to provide you with the fundamentals of the GENESIS32 Automation Suite. You will become comfortable with OPC architecture and GENESIS32 modules including: GraphWorX32, AlarmWorX32, TrendWorX32, Workbench32, Aliasing, Unified Data Manager, Security, creating Web-based applications, Enterprise Reporting, Charting and Analysis as well as the use of Multimedia Alarm notification, all in a secure GENESIS32 environment. Emphasis is placed on SCADA (Supervisory Control and Data Acquisition) and HMI (Human Machine Interface) aspects of the product. The course is designed to provide you with a good working knowledge of and the ability to configure, operate and maintain a GENESIS32 system.	40 hours	$3,000				Novice
GENESIS64 + Dashboards	The GENESIS64 + Dashboards course is a 5-day, instructor-led class. The course is designed to provide students with a good working knowledge of the GENESIS64 Application Server and dashboards. All major features are covered from project configuration to data acquisition, visualization and deployment. Valuable hands-on lab exercises guide you through building and modifying the HMI/SCADA platform. This course also provides in-depth understanding of visualization for your facility data using dashboards, GraphWorX64 advanced features, Commanding and GEO SCADA mapping technology of EarthWorX. Specific ICONICS products used during this course include: GraphWorX64 for visualization, AssetWorX64, AlarmWorX64, TrendWorX64, ReportWorX Express and PortalWorX.	40 hours	$3,000				Intermediate
GENESIS64 Hyper Historian	The GENESIS64 + Hyper Historian course is a 5-day, instructor-led class. This course is designed to provide students with a good working knowledge of the GENESIS64 Application Server and Hyper Historian. All major features are covered from project configuration to data acquisition, visualization and deployment. Valuable hands-on lab exercises guide you through building and modifying the HMI/SCADA platform. This course also provides fundamental design philosophy and concepts of Hyper Historian. The student will configure OPC, BACnet, database and other data points for collection, compression and storage. Learn how to utilize Hyper Historian performance calculations for custom data processing and how to visualize and report the results. Specific ICONICS products used during this course include: GraphWorX64, AssetWorX64, AlarmWorX64, TrendWorX64, Hyper Historian and ReportWorX Express.	40 hours	$3,000				Intermediate
Building Basic Displays with PI Process Book	In this course, we will guide you on how to create a variety of PI ProcessBook displays, such as trends and bar graphs, to monitor your process. Additionally, this course leverages the power of the intuitive PI AF asset structures to enable you to display attributes of an asset, search in AF, and build element relative displays.	16 hours	$159				Intermediate
Visualizing PI System Data with PI Vision	Learn how to build dynamic, graphical, interactive web-based dashboards with PI Vision. This self-paced online course is dedicated to a series of exercises where the student is challenged to solve real-world problems using PI Vision.	24 hours	$1,625				Intermediate

Enabling Condition Based Maintenance	The objectives of the course are to help your organization eliminate unnecessary maintenance, minimize unexpected failures, maximize use of resources, increase reliability and availability, and extend the lifetime of various assets using the OSIsoft PI System. In this course, you will learn how to use AF templates, Event Frames and Asset Analytics to implement advanced logic to evaluate your equipment's health, as well as how to use Notifications to receive automated alerts based on deviations in your process data. Additionally, you'll see how easy it is to use tools like PI Vision and PI DataLink to visualize important information about your equipment and make informed maintenance decisions.	16 hours	$159				Intermediate
Analyzing PI System Data	The Analyzing PI System Data course is focused on analyzing PI System data through Business Intelligence (BI) and reporting tools. The class will cover aspects of the following tools: The new RTQP Engine (PI SQL Client), PI Integrator for Business Analytics, Microsoft Excel, Microsoft Power BI, and SQL Server Reporting Services (SSRS) Report Builder. If you feel like writing business reports is too difficult, this may be the course for you. We will build upon your existing application knowledge with hands-on activities to help you transform data into information.	24 hours	$1,400				Advanced
Introduction to Cyber Security			$0 - $89				Fundamentals
Cyber Security Operations			$89	Online			Intermediate
Cybersecurity Policy for Water and Electricity Infrastructures				Online			Fundamentals
Cybersecurity Policy for Aviation and Internet Infrastructures				Online			Fundamentals
Enterprise and Infrastructure Security				Online			Novice
Cyber Security in Manufacturing				Online			Novice
Introduction to Cybersecurity Tools & Cyber Attacks				Online			Novice
Cybersecurity Roles, Processes & Operating System Security				Online			Novice
Cybersecurity Compliance Framework & System Administration				Online			Novice
Network Security & Database Vulnerabilities				Online			Novice
Access Controls				Online			Intermediate
Security Operations and Administration				Online			Intermediate
Identifying, Monitoring, and Analyzing Risk and Incident Response and Recovery				Online			Intermediate
Cryptography				Online			Intermediate
Networks and Communications Security				Online			Intermediate
Systems and Application Security				Online			Intermediate
The CISM Exam Review Class		8 weeks	$2,295	Online with live broadcast			Design
Assessing, Hunting, and Monitoring ICS Networks		5 days	$4,500	Live			Design

Table 1: 'Trainings' spreadsheet in Randall Jung's repository of cybersecurity courses.

```
Document: Is a high level introductory course designed to expose participants to the challenges and frameworks used in implemen
ting and sustaining a cyber security program at a nuclear and/or radiological facility.  The course uses the National Institute
of Standards and Technology (NIST) cyber security framework as the course structure for conveying the core concepts and compone
nts of a cyber security program.  This includes, identifying sources of risk, protection of digital systems, detection concepts
should protection fail, response to detection points, and recovering the system back to conditions before a cyber event.
Similar Documents:

Out[28]: {'roles': ['ovmgt001 : 60.22%',
  'prcda001 : 51.55%',
  'sprsk001 : 50.87%',
  'spsys001 : 50.84%',
  'sprsk002 : 49.65%',
  'prcir001 : 49.18%',
  'sparc002 : 48.75%',
  'omana001 : 48.18%',
  'ovexl001 : 45.98%',
  'sparc001 : 45.09%',
  'spsys002 : 43.16%',
  'coopl003 : 42.67%',
  'coopl002 : 40.74%',
  'spdev002 : 40.55%',
  'ovspp002 : 38.67%',
  'ovtea002 : 38.25%',
  'prinf001 : 38.2%',
  'ovspp001 : 37.79%',
  'ovmgt002 : 36.0%',
  'spdev001 : 35.83%',
  'ovtea001 : 35.61%',
  'coopl001 : 35.46%',
  'ovpma001 : 34.06%',
  'spsrp001 : 33.88%',
  'ovpma005 : 33.79%',
  'sptrd001 : 32.1%',
  'antgt002 : 31.82%',
  'prvam001 : 31.02%',
  'ovpma002 : 30.37%',
  'anasa002 : 30.29%',
  'omadm001 : 29.6%',
  'infor002 : 29.43%',
  'antgt001 : 29.27%',
  'omsts001 : 29.23%',
  'anasa001 : 28.62%',
  'ovpma003 : 27.95%',
  'infor001 : 27.22%',
  'omnet001 : 26.86%',
  'coops001 : 26.86%',
  'anexp001 : 26.23%',
  'antwa001 : 25.57%',
  'ovpma004 : 25.23%',
  'sptst001 : 24.92%',
  'ovlga002 : 24.83%',
  'ininv001 : 23.36%',
  'ovlga001 : 20.66%',
  'omdta001 : 19.24%',
  'omkmg001 : 18.8%',
  'omdta002 : 16.66%',
  'anlng001 : 16.11%',
  'coclo001 : 9.84%',
  'coclo002 : 9.06%']}
```

Figure 1: Example of NICE Work-roles attributed to an input document (course description) with Cosine Similarity as percent match included.

```
In [1]: import b_script

In [2]: course = 'Is a high level introductory course designed to expose participants to the challenges and frameworks used in implement
```

Input

"Is a high level introductory course designed to expose participants to the challenges and frameworks used in implementing and sustaining a cyber security program at a nuclear and/or radiological facility. The course uses the National Institute of Standards and Technology (NIST) cyber security framework as the course structure for conveying the core concepts and components of a cyber security program. This includes, identifying sources of risk, protection of digital systems, detection concepts should protection fail, response to detection points, and recovering the system back to conditions before a cyber event."

Output

```
In [3]: b_script.analyze(course)

Out[3]: {'compLevel': 'Novice',
 'roles': ['ovmgt001 : 60.22%',
  'prcda001 : 51.55%',
  'sprsk001 : 50.87%',
  'spsys001 : 50.84%',
  'sprsk002 : 49.65%',
  'prcir001 : 49.18%',
  'sparc002 : 48.75%',
  'omana001 : 48.18%',
  'ovexl001 : 45.98%',
  'sparc001 : 45.09%',
  'spsys002 : 43.16%',
  'coopl003 : 42.67%',
  'coopl002 : 40.74%',
  'spdev002 : 40.55%',
  'ovspp002 : 38.67%',
  'ovtea002 : 38.25%',
  'prinf001 : 38.2%',
  'ovspp001 : 37.79%',
  'ovmgt002 : 36.0%',
  'spdev001 : 35.83%',
  'ovtea001 : 35.61%',
  'coopl001 : 35.46%',
  'ovpma001 : 34.06%',
  'spsrp001 : 33.88%',
  'ovpma005 : 33.79%',
  'sptrd001 : 32.1%',
  'antgt002 : 31.82%',
  'prvam001 : 31.02%',
  'ovpma002 : 30.37%',
  'anasa002 : 30.29%',
  'omadm001 : 29.6%',
  'infor002 : 29.43%',
  'antgt001 : 29.27%',
  'omsts001 : 29.23%',
  'anasa001 : 28.62%',
  'ovpma003 : 27.95%',
  'infor001 : 27.22%',
  'omnet001 : 26.86%',
  'coops001 : 26.86%',
  'anexp001 : 26.23%',
  'antwa001 : 25.57%',
  'ovpma004 : 25.23%',
  'sptst001 : 24.92%',
  'ovlga002 : 24.83%',
  'ininv001 : 23.36%',
  'ovlga001 : 20.66%',
  'omdta001 : 19.24%',
  'omkmg001 : 18.8%',
  'omdta002 : 16.66%',
  'anlng001 : 16.11%',
  'coclo001 : 9.84%',
  'coclo002 : 9.06%']}
```

Figure 2: Working example of model classification and output.

Securely Provision (SP) Risk Management (RSK)	**Authorizing Official (SP-RSK-001)**: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).	Click to view the Master KSA List Click to return to the Table of Contents
		OPM 611
KSA ID	**Knowledge**	
	Knowledge	
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	
K0004	Knowledge of cybersecurity and privacy principles.	
K0005	Knowledge of cyber threats and vulnerabilities.	
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.	
K0019	Knowledge of cryptography and cryptographic key management concepts	
K0027	Knowledge of organization's enterprise information security architecture.	
K0028	Knowledge of organization's evaluation and validation requirements.	
K0037	Knowledge of Security Assessment and Authorization process.	
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	
K0048	Knowledge of Risk Management Framework (RMF) requirements.	
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	
K0084	Knowledge of structured analysis principles and methods.	
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	
K0146	Knowledge of the organization's core business/mission processes.	

Table 2: Reference spreadsheet from the Workforce Framework for cybersecurity.

Appendix D – External Programs

MIT-INL AI/ML 2021 Summer Symposium:

We enrolled in and attended INL and MIT's collaborative Artificial Intelligence/Machine Learning 2021 Summer Symposium. Through the symposium lectures we were able to get a better grip on Python basics, latest Machine Learning libraries and packages, as well as an overall deeper understanding of AI/ML concepts and theories.

Intern Enrichment Series:

We took part in N&HS' Intern Enrichment Series in which we were able to get better acquainted with INL and the many branches INL's work touches by engaging with speakers who shared their unique experiences in their respective fields.

2021 Intern Poster Session:

We submitted a poster to INL's Intern Poster Session in which our project is to be displayed at a high level for any interested party to observe.

ISCOP Briefings:

We had a chance to get feedback directly from industry professionals via biweekly ISCOP briefings. The comments we received were very insightful and helped us improve the way we communicate our project and problem statement.

CISA VLP Courses:

We were enrolled and completed the 100W, 210, 301V, and 401V training courses offered by CISA through the VLP. These courses introduced us to concepts within ICS cybersecurity, as well as the consequences and different relationships ICS has to IT and OT.